科学研究費補助金 特定領域研究

新世代の計算限界
— その解明と打破 —

平成16年度 成果報告書

平成17年 4月

領域代表者　岩間 一雄
京都大学 大学院 情報学研究科　教授

目 次

1. 総括班活動報告 **1**
活動の概略 . . . 3
教科書シリーズ . . . 5
ジャーナル刊行 . . . 5
ニュースレター . . . 6
NHC 国際会議 . . . 8
電子情報通信学会 2005 年総合大会チュートリアル講演「計算限界の中心で解法を叫ぶ」 . . . 12
第 18 回 回路とシステム軽井沢ワークショップ講演企画 . . . 13
ランダムネスと計算 (特定領域「確率的情報処理」との共同開催) . . . 14
ミニ研究集会 (研究の種をいかに育てるか) . . . 15
ミニ研究集会 (グラフアルゴリズム) . . . 16
ミニ研究集会 (量子計算) . . . 17
ミニ研究集会 (論理関数) . . . 18
ミニ研究集会 (列挙アルゴリズム) . . . 20

2. 研究課題別活動報告 **21**
A01: オンライン予測の手法を用いた意思決定モデルに関する研究 . . . 23
A02: 計算理論的設計による知識抽出モデルに関する研究 . . . 32
A03: 論理関数表現のモデルとシンボリックアルゴリズム . . . 44
A04: 組み合わせ最適化における指数サイズ・多項式時間近傍の設計 . . . 52
A05: ハードウェアアルゴリズムの性能評価に関する研究 . . . 62
A06: 幾何的配置問題の計算量限界と近似可能性の研究 . . . 70
A07: 現実的な状況下での量子計算の能力に関する研究 . . . 78
A08: 動的な構造をもつネットワーク上の資源割当て問題の研究 . . . 88
A09: 非明示的表現に対するアルゴリズムの開発 . . . 100
A10: 変移する要素間の関係を条件とする組合せ最適化モデル . . . 110
B01: 代数的および確率的手法による離散構造の限界の究明 . . . 118
B02: 暗号解析手法の計算量理論による改良とそれに基づく暗号方式 . . . 130
B03: 量子論理回路の最適化に関する研究 . . . 140
B05: ブール理論に基づく離散システムの構造解析と計算限界の研究 . . . 151
B06: 暗号システムに対する実装攻撃の適用と限界に関する計算的研究 . . . 159
C01: グラフ描画アルゴリズムとその Web 情報検索への応用 . . . 170
C02: 連続と離散の統合によるロバストアルゴリズム構築 . . . 182
C03: ネットワーク上での社会的効用と個人的効用の対立問題に対するアルゴリズム的研究 . . . 204
C04: 実践的な列挙アルゴリズムの理論構築 . . . 214
C05: 幾つかの画像関連問題の計算複雑度の解析と効率的な解決法の提案 . . . 223
C06: グラフ構造を有する問題に対する近似アルゴリズムの設計 . . . 243

C07: Web コンテンツ活用に関連した離散最適化問題の研究 255
C08: 高性能近似アルゴリズムの設計法に関する研究 265
C09: ネットワーク問題のモデル化とアルゴリズムの研究 273
C10: 情報基盤アルゴリズムとしてのメタヒューリスティクスの研究 293
C11: 大量データ処理のための領域効率の良いアルゴリズム 309

3. 各種資料 **315**
ニュースレター 第 1 号 317
ニュースレター 第 2 号 325
平成 16 年度 第 1 回 全体会議 講演資料 330
Proceedings of the Workshop on New Horizons in Computing 337
The Workshop on New Horizons in Computing 講演資料 396

1. 総括班活動報告

1　活動の概略

今年度は，国際会議１件，電子情報通信学会のチュートリアル企画１件，ミニ研究集会５件，全体会議１件，幹事会３件のように集会を行った．さらに計画中の集会として，特定領域研究「確率的情報処理」との合同研究集会と，電子情報通信学会の回路とシステム軽井沢ワークショップでの招待講演セッションがある．そして海外からの６名研究者を招聘（上記の国際会議の招待講演者を除く）し，ポスドクを１名雇用した．また，会員間の情報交換のためのニュースレターの発行を開始した（2004 年度は２号発行）．その他には，教科書シリーズやジャーナルの発行の可能性を探って出版社などと交渉を開始している．それぞれの概要を以下で説明し，必要に応じて詳細を次節以降に記す．なお，全体会議と幹事会の詳細は，ニュースレターを参照のこと．

国際会議

本特定領域研究の主催で，以下の国際会議を開催した．

会議名 Workshop on New Horizons in Computing — Recent Trend in Theoretical Computer Science

日程 2005 年 2 月 28 日〜3 月 3 日

場所 京都ロイヤルホテル（京都市中京区河原町三条上る）

内容 招待講演 21 件（うち外国人 19 名）と一般講演 8 件

参加者 約 140 名

チュートリアル企画

電子情報通信学会 2005 年総合大会においてチュートリアル企画を行った．

企画名 計算限界の中心で解法を叫ぶ

日時 2005 年 3 月 23 日 13 時〜17 時

場所 大阪大学 豊中キャンパス

内容 第一部：講演 4 件．第二部：問題相談コーナー（全６ブース）

軽井沢ワークショップ企画（計画）

本特定領域研究の広報などのために，第 18 回 回路とシステム軽井沢ワークショップにおいて招待講演を計画している．

日時 2005 年 4 月 26 日 9:30〜12:00

場所 軽井沢プリンスホテル 西館

合同研究集会（計画）

特定領域研究「確率的情報処理」との共同開催の研究集会「ランダムネスと計算 (Randomness and Computation)」を計画している．

日程 2005 年 7 月 18 日〜22 日

場所 仙台国際センター

ミニ研究集会

研究を活性化するために，テーマ毎のミニ研究集会を奨励した．以下の５件が実施された．

「研究の種をいかに育てるか」

2005 年 3 月 12 日, 北陸先端科学技術大学院大学

「グラフアルゴリズム」

2005 年 3 月 19 日, 日本大学 文理学部

「量子計算」

2005 年 3 月 26 日, 電気通信大学

「論理関数」

2005 年 3 月 28 日, 九州工業大学 天神サテライトキャンパス

「列挙アルゴリズム」

2005 年 3 月 29 日〜31 日, 群馬大学 伊香保研修所

全体会議

日時 2004 年 10 月 13 日　13 時 50 分〜17 時 30 分

場所 東北大学

内容 講演（キーノートスピーチ）２件

- 永持仁 (京都大学): Approximation Algorithms for the Minmax Subtree Cover
- 青木孝文 (東北大学): 位相情報を用いた画像マッチングとその応用— ピクセルとピクセルの間をみる技術 —

全体討論

幹事会

本特定領域研究は，総括班に数名加えた幹事団によって運営される．本年度は幹事会を３回の幹事会を行った．

メンバー (17 名) 浅野孝夫（中央大），浅野哲夫（北陸先端大），伊藤大雄（京大），岩間一雄（京大），宇野毅明（国立情報学研究所），加藤直樹（京大），櫻井幸一（九大），杉原厚吉（東大），瀧本英二（東北大），田中圭介（東工大），徳山豪（東北大），西関隆夫（東北大），平田富夫（名大），堀山貴史（京大），牧野和久（阪大），山下雅史（九大），渡辺治（東工大）．

第１回 2004 年 7 月 27 日 17 時〜20 時, 京都大学

第２回 2004 年 10 月 13 日 12 時〜13 時 40 分, 東北大学

第３回 2005 年 3 月 2 日 20 時〜21 時, 京都ロイヤルホテル（兼 国際会議ビジネスミーティング）

教科書・ジャーナル

人材の育成としての教科書シリーズの発行，研究成果発表の場としてのジャーナルの発行の可能性を探るため，担当者を決め検討を開始した．初年度は色々な可能性を探っている段階である．

ニュースレター

会員間の情報交換のため，年４回発行を目指して発行が開始された．新年度は年度途中からなので 11 月に第１号，3 月に第２号が発行された．

招聘研究者

以下の研究者を招聘した．なお，*印は国際会議の招待講演者でもある．

1. Susanne Albers (University Freiburg), 2005.2.26–2005.3.5 *
2. Wolfgang Bein (University of Nevada, Las Vegas), 2004.12.11–2005.1.15
3. Avrim Blum (Carnegie Mellon University), 2005.2.21–2005.3.5 *
4. Timothy Chan (University of Warterloo), 2005.2.26–2005.3.3 *
5. Richard Cole (New York University), 2005.2.26–2005.3.5 *
6. Josep Diaz (Universitat Politecnica de Catalunya), 2005.2.22–2005.3.5 *
7. Peter Eades (University of Sydney), 2005.2.27–2005.3.31
8. Herbert Edelsbrunner (Duke University), 2005.2.26–2005.3.4 *
9. Martin Farach-Colton (Rutgers University), 2005.2.23–2005.3.3 *
10. Uriel Feige (the Weizmann Institute), 2005.2.26–2005.3.6 *
11. Lisa Fleischer (IBM), 2005.2.26–2005.3.5 *
12. Lance Fortnow (University of Chicago), 2005.2.25–2005.3.4 *
13. Seok-Hee Hong (University of Sydney), 2005.3.9–2005.3.21
14. Tao Jiang (University of California-Riverside), 2005.2.26–2005.3.4 *
15. Oded Lachish (Haifa University), 2005.1.26–2005.2.18
16. Ming Li (University of Waterloo), 2005.2.27–2005.2.28 *
17. Andrezj Lingas (Lund University), 2005.1.26–2005.2.28

18. Jiri Matousek (Charles University, Prague), 2005.2.28–2005.4.8 *
19. Shan Muthukrishnan (Rutgers University), 2005.2.26–2005.3.5 *
20. Seffi Naor (Technion Israel Institute of Technology), 2005.2.26–2005.3.5 *
21. Saidur Rahman (Bangladesh University of Engineering and Technology), 2004.12.22–2005.3.11
22. R. Ravi (Carnegie Mellon University), 2005.2.25–2005.3.6 *
23. David B. Shmoys (Cornell Universityq), 2005.2.26–2005.3.2 *
24. Mikkel Thorup (AT&T), 2005.2.19–2005.3.4 *
25. Uri Zwick (Tel Aviv University), 2005.2.21–2005.3.21 *

ポスドク

若手の支援と育成のためにポスドクを雇用する．本年度は１名の採用を行った．

氏名 稲永俊介

期間 2005 年 1 月 1 日〜3 月 31 日

機関 九州大学

2　教科書シリーズ

担当者：　杉原厚吉 (東京大学)，室田一雄 (東京大学)，山下雅史 (九州大学)，渡辺治 (東京工業大学)

本特定領域がカバーしようとしている計算の分野の重要性とおもしろさを伝えるとともに，この分野の次世代を背負う人材の養成に役立つ体系的な教科書作りをめざして検討を始めた．幸い，共立出版 (株) が，本企画に協力していただけることになった．共立出版の編集部とともに，2004 年 12 月 22 日，2005 年 1 月 31 日，2 月 1 日，3 月 11 日に編集会議を開き，次のような概要を固めた．

本教科書シリーズ名は「アルゴリズム・サイエンス　シリーズ」とする．

時代の要請として，次の三点を特に意識して編成を考える：(1) 並列計算機や分散計算環境が容易に手に入る時代となり，このような新しい計算環境を生かして問題を解決するための新しい解法が必要とされている；(2) バイオインフォマティックスやナノ技術など多くの応用分野が巨大な問題を上手に扱うための新しい計算パラダイムを必要としている；(3) 情報セキュリティという重要な応用分野の出現によって，従来は応用に乏しい理論研究と考えられていた整数論や計算困難性理論が実学として期待されるようになった．

これらの時代要請を踏まえた上で，広い読者層に対応できるよう，シリーズ全体の構成を次の 3 階層とする．

1. 若い人へ「アルゴリズム」に対する興味・関心・問題意識を喚起するもの（入門編：大学１，２年生が主対象）．理論や手法を手がかりとした「入口からの超入門」と，応用分野の話題を手がかりとした「出口からの超入門」の２編構成とする．
2. 基本的手法あるいは今まで取り上げられていない興味深い手法をわかりやすく解説するもの（手法編：大学３，４年生が主対象）.「分散アルゴリズム」,「確率アルゴリズム」,「オンラインアルゴリズム」などを含めて７編程度の構成とする．
3. 注目度の高い具体的な問題に結びつけて，研究へのモチベーションを高めるもの（応用編：学部上級から大学院生が主対象）．バイオインフォマティックス，データマイニングなど４，５編の構成とする．

以上のような基本方針を固め，現在，具体的な各編の構成と執筆者の決定作業を行っている．入門編の２冊は，2005 年 9 月末脱稿，その他は 2006 年 3 月末脱稿をめざし，順次発行していく予定である．

3　ジャーナル刊行

担当者：　徳山豪 (東北大学)

本特定領域研究の研究成果の発表の場として，新しいジャーナルの刊行を行う事の是非について，

平成 16 年 10 月 13 日の全体会議で討論を行った．現状では，本特定領域研究の主要なメンバーは主に海外の一流紙に英文で発表しており，また，学生の論文発表の場も整備されているという状況であることから，通常の印刷体としてのジャーナルを新規に発足させる事にはメリットが少なく，またプロジェクト終了後の継続性にも問題がある．更に情報科学のプロジェクトとしては，現代的な電子媒体による情報交換を考えるほうが自然であり，実用的である．従って，主に速報的な電子ジャーナルもしくはプレプリントのアーカイブシステムとしての実現性について意見交換を行った．

特にプレプリントのアーカイブシステムについては海外で様々のシステムがあるが，日本の当分野では公式のものは無いので，実現性についての検討を行う担当者（東北大学，徳山）を決めた．
要望が多数ないと実現のメリットが無いのと同時に多くのメンバーが自発的にプレプリントを提出するという条件が必須であるので，メンバーからの要望や意見を担当者の元に集計するという事となった．また，著作権や継続性等についての問題，検索や保守，情報管理・セキュリティーなどデータベースとしてのシステム構築の費用や手間についての検討も行う．　要望によりアーカイブシステムを実現する場合は，まずは非公式の実験システムとして平成 17 年度に開始する予定である．

4　ニュースレター

担当者：　宇野毅明 (国立情報学研究所)，　牧野和久 (大阪大学)

ニュースレターは，特定領域・新世代の計算限界のメンバーの情報交換と交流を目的とした情報発信誌となるべく企画された．近年，個別の研究成果に関しては多くの情報が簡単に手に入るようになったが，その裏に隠れている，研究者の思想や，研究推進のノウハウ，基礎的なアイディアといった点については，目に付かずに隠れている場合が多い．具体的は，研究のゴールどこに設定しているか，この理論のアイディアはどのあたりからどのように設定していたのか，この研究において主観的に評価の高いところはどこであるか，今後どのようなテーマがありうるか，応用，他分野などからの反応，問われている必要性はどのようなものであるか，といった点である．このような事柄を広く研究者間で共有することは，日本のアルゴリズム研究の全身のためになくてはならないことである．しかし，現時点でこのような情報を効率良く収集することは，それほど容易なことではなく，各研究者の個人的なつながりを中心として細々と行われているにとどまっている．

ニュースレターは，このような研究者間の情報交換を促進させることを目的として企画された．年 3-4 回の発行を行い，毎回，いくつかの研究関連の記事と，特定領域のスケジュール・活動報告と，各研究者の活動予定などを掲載する．本年度は，第 1 号を 11 月初旬に，第 2 号を 3 月初旬に発行した．

各号は電子メールで配布を行う．短い記事や連絡事項は全て掲載するが，長い記事，イベントの詳細などは web ページに掲載し，簡便に閲覧できる電子メール媒体と，詳細を効率よく閲覧できる web ページにてお互いを補完する．web 版は，現在

http://keisan-genkai.lab2.kuis.kyoto-u.ac.jp/newsletter/news1.html
http://keisan-genkai.lab2.kuis.kyoto-u.ac.jp/newsletter/news2.html

に掲載してある．

情報交換のため，各号に１つ，2000-4000 字程度研究に関わる記事を掲載する．これは，１つの研究課題が担当する．通常，このようなニュースレターでは，研究成果を報告するのが一般的であるが，この特定領域では「研究者の交流」に焦点を当てたいため,「研究の成果以外」の記事を，面白く解説する．例えば，最近参加した国際会議の情報を，どのようなものが流行っていたか，何が面白かったか，などの主観的な解説を交えて報告したり，最近考えている問題，あるいはオープン問題を，この辺までは解けるがここがうまくいかない，といった解説を交えて紹介する，という形である．

また，研究者間の交流を促進するため，各研究者の，国内外の会議への出席予定を集約して掲載する．研究者の交流には，顔をあわせる回数を増やすことが肝要であり，他の研究者の参加予定が

わかれば，会議への出席のモチベーションを高め，ディスカッションや研究成果を生むきっかけにもなる．

以下に，今年度発行した第 1 号・第 2 号について，それらの目次を示す．

第 1 号目次:

1. 特定研究「新世代の計算限界」のスタートに当って
　　— 岩間 一雄 (京都大学)
2. 特定領域研究「新世代の計算限界」の発足を祝う
　　— 稲垣 康善 (愛知県立大学)
3. 寄稿: An introduction to the puzzle of European research funding — Josep Diaz
　　(スペイン・カタロニア工科大学)

４．2004 年度第 2 回幹事会・第 1 回全体討論概要
　　— 事務局

５．イベントカレンダー

第 2 号目次:

1. ボロノイ図とその応用国際シンポジウムを開催して
　　— 杉原厚吉 (東京大学)
2. NHC Workshop Business Meeting (兼 2004 年度第 3 回幹事会) 議事録 — 事務局
3. イベントカレンダー ＋ 事務連絡
4. このニュースレターについて

NHC国際会議

担当者:　岩間一雄 (京都大学)，徳山豪 (東北大学),
Magnus Halldorsson (アイスランド大学),
伊藤大雄，堀山貴史 (京都大学)

1　会議のあらまし

本特定領域研究のキックオフ国際会議として，平成 15 年 2 月 28 日から 3 月 3 日の 4 日間，京都市京都ロイヤルホテルにおいて Workshop on New Horizon in Computing – Recent Trend in Theoretical Computer Science (略称：NHC 国際会議) を開催した．　岩間一雄（京都大学）を会議委員長とし，徳山豪（東北大学）と Magnus Halldorsson（アイスランド大学）がプログラム作成，伊藤大雄，堀山貴史（京都大学）がローカルアレンジ，を担当した．

招待講演者として，Susanne Albers (Freiburg), Avrim Blum (CMU), Timothy Chan (Waterloo), Richard Cole (NYU), Josep Diaz (UPC), Herbert Edelsbrunner (Duke), Martin Farach-Colton (Rutgers), Uriel Feige (Weizmann), Lisa Fleischer (IBM), Lance Fortnow (Chicago), Tao Jiang (UC Riverside), Ming Li (Waterloo), Kazuhisa Makino (Osaka) Jiri Matousek (Charles), S. Muthukrishnan (Rutgers), Seffi Naor (Technion), R. Ravi (CMU), David Shmoys (Cornell), Mikkel Thorup (AT&T) , Osamu Watanabe (Tokyo Inst. Tech.) ,Uri Zwick (Tel-Aviv) の 21 人の世界最前線の研究者にそれぞれ 50 分の講演を依頼し，その他，8 件の日本人講演者による 20 分講演（Short Talk）と，2 回の Discussion セッション（計 3 時間）及び今後の国際交流計画に関するビジネスミーティングを行った．4 日間とも朝 8 時 40 分開始というスケジュールで密度の高い討議が行われた．参加者は，海外からの聴衆も含め，約 140 人であり，学生の参加者も多数であった．招待講演者にはそれぞれ下記のような会議の目的に賛同して講演を準備してもらい，計算限界への挑戦のための様々なモデルや手法について，研究の動機・歴史と共に最新の進展の紹介が行われた．

2　会議の目的

本国際会議の主たる目的は,「理論的な計算限界によるさまざまな困難を解明し打破する」という特定領域研究の目標への最先端アプローチの調査と，世界的な共同研究体制の構築である．具体的には世界的に進んでいる様々な新しい理論モデルや計算理論の最先端を，最前線の研究者の講演によって紹介し，更に彼らとの討議により，本特定領域研究の研究者の考えているモデルや理論への新しいアイデアの導入や意見交流を図るものである．なお，英文で WEB 上で公開し世界に発信した，より詳細な会議の Objective は下記（一部抜粋）のものである．

The category of intractable (typically NP-hard) problems includes great many problems of fundamental and practical importance. When we encounter such a problem, we are forced to try to solve it in some way within a reasonable amount of time. This is generally bound to lead to a sacrifice on the optimality of the solution. In that case it is much preferable to be able to use an algorithm for which we know the maximum amount of this sacrifice mathematically or whose performance is rigorously guaranteed. In the past two decades, researchers have spent a lot of effort towards this goal, i.e., studying how to guarantee the performance of combinatorial optimization algorithms. Fortunately our level of knowledge on this topic has dramatically improved.　（中略）

This line of research has recently been expanded into several interesting directions, providing new models for the design and analysis of contemporary algorithms, such as those for property testing, lattice problems, extraction, drawing, meta heuristics, truthful auction, web

graphs, data mining, and many more. These new trends are still emerging and the situation is rapidly changing. To capture these many new exciting opportunities for our research community, a new theory project, "New Horizons in Computing" funded by the Ministry of Education in Japan for the next four years, has started in September 2004.

The NHC workshop is to kick off this project, consisting of some 20 invited talks by world-leading researchers. These will illustrate cutting-edge research, explore current trends, and glimpse future visions in theoretical computer science.

3 会議の内容

第一線の研究者たちの講演はどれも熱気に溢れていたが，特に招待講演に関してトピックを分類して，簡単に内容を紹介する．

計算生物学における新しいモデルと進展

計算生物学は遺伝子解析に欠かせない分野である．Ming Li による講演では，Kolmogorov 計算量のバックグラウンドから生じたアイデアを用いて彼らの開発した PatternHunter アルゴリズムが紹介された．手法のキーポイントは最適にスペースの空いたシードパターンを用いる事にあり，現在遺伝子の類似探索に用いられる Blast アルゴリズム（スペースの無いシードパターンを用いる）を理論・実用両面で凌駕する．T. Jiang による講演は半遺伝子型（たとえば，血液型の A 型表示の半遺伝子型は AO または AA) の推定であり，家系（の一部）の遺伝子型データから半遺伝子型を推定する手法の最先端研究が紹介された．更に,H. Edelsbrunner は，計算幾何学の一分野として最近注目されている計算位相幾何学において，物体（多様体）からサンプルされた点集合から元の物体の位相（ホモロジー）を推定する問題を取り上げ，その計算生物学（プロテインマッチング）への応用の解説を行った．

Stochastic Optimization のモデルと解析

組合せ構造を構築する時，データがオンラインに入力され，過去に作成した構造に追加する形で構築する問題（オンライン問題）は十数年ほど盛んに研究されてきたが，モデルとして実用性に疑問視される面があった．これに対し，データが何段階かに分けて入力され，かつ，将来のデータ入力がいくつかの仮想モデルから統計的に選ばれるというモデル（Stochastic Optimization モデル）がより現実的なモデルとして近年考案されている．統計情報は，小規模なサンプルを数回取って推定する．特にデータが 2 段階に入力される場合を中心に，最初のステージでのデータ構築が 2 番目のステージでのデータ構築よりも安価であるという仮定の元でシュタイナーネットワーク問題や施設配置問題を例にして具体例と手法の概説と広範囲の応用や研究現状を R. Ravi が，数理計画法によるより詳細なアプローチを D. Shmoys が解説した．Stochastic Optimization については，モデル自体が確立しているとは言えず，質疑や討議においても，今後の研究課題が多いという印象であった．

巨大データ・ストリームデータのアルゴリズム

メインメモリに載らない巨大なデータを処理するときに，外部記憶へのアクセス回数を減らす計算モデルの研究として，ストリーム型アルゴリズム（データは巨大な配列で，逐次読み取りを行うモデル）とキャッシュオブリビアスアルゴリズム（外部データはブロックでメインメモリにキャッシュされるが，ブロックサイズや外部データへのアクセス時間などのパラメタは与えられていない計算モデル）の最先端の研究が紹介された．T. Chan の講演は，幾何学データ処理に対するストリーム型アルゴリズムがテーマであり，良く知られた中央値問題や幾何学的中心点問題に対しても， ストリームデータの場合では新しい技法が必要になることを示し，計算幾何学での新しい分野の出現を印象付けた．S. Muthukrishnan の講演はインターネットのアクセスデータから不正アクセスを検出する問題を例にしたストリーム型アルゴリズムであり，講演の冒頭に示したパズル問題などへの反応など活発な意見交換を生んだ．M. Farach Colton の講演はキャッシュオブリビアスモデルと，従来の 2 次記憶モデルの比較に関する講演であった． 現実の汎用計算機モデルでの大規模データ処理における適切な理論モデルである事を実験を交えて証明してみせた．

非協調システムの均衡制御のアルゴリズム

インターネットや経済などの非協調な成長・競合システムの理論解析は近年のホットトピックである．R. Cole の講演では，カリフォルニアにおける高速道路の渋滞解消のための動的な通行料の設定から始まり，インターネットにおける「6 分離次数」（メール等の情報伝達が高々6 つの中継地点で実現できる）の性質のモデル化，商取引における価格均衡理論などをテーマに，非協調分散プロセスや非協力ゲームのパラメトリックなコントロールに共通する計算理論的な諸概念の紹介や問題提起が行われた．L. Fleisher の講演でも同じ高速道路の通行料の例が示され, 非協力ゲームを用いた価格均衡理論での近似ナッシュ均衡の計算理論と，均衡状態の改善のための制御理論がテーマとなった．S. Albers は，巨大ネットワークのバッファマネジメントや WEB キャッシングのモデル化と近似アルゴリズム設計理論及びインターネットの生成プロセスの理論を紹介した．

機械学習・推論の最先端

A. Blum の講演では，まずインターネット上でのスパムの分類（Muthucrishnan の講演でも紹介された）を例にとって，高次元空間でのデータ分離として機械学習を述べ，良く知られた PAC 学習を超える理論を目指すために提唱されている機械学習の最近の主要問題を概説した．特に非線形分離サポートベクトルマシンの設計で，類似度を表すカーネル関数を巨大次元空間の内積と捉えて低次元に射影する手法と解析について紹介した．牧野和久は，論理の補完列挙において，従来の予想を覆す多項式遅延列挙アルゴリズムとその周辺を紹介した．例えば，“車がパンクした” という帰結に対して，“車が動かなくなった” という現在の前提条件に付加して帰結を確定的に示す補完する仮説（例として “エンジンは動いている” かつ “パンという音がした”）の列挙を行う問題であり，AI や発見科学での大きな問題である．帰結の種類に応じて計算クラスが著しく変る事実を示し，計算理論の貢献が重要である事を強調した．

最適化問題に対する最新の進展

最適化問題に関して統一的な取り扱いを行うモデルの提案は大きなテーマであるが，J. Matousek は線形計画法の組合せ最適化としての一般化について最新の成果と計算限界を紹介した．マトロイド理論との関連や，強多項式線形計画法アルゴリズムの設計の困難さとの関連や，計算幾何学での手法の一般次元への拡張の試みなどが論じられた．S. Naor はグラフ上の様々な問題をモデル化する距離ラベル問題について，定式化と近似アルゴリズムの最先端の理論を展開した．

ネットワークアルゴリズムの進展

ネットワークやグラフのアルゴリズムは計算理論の古典的なテーマであるが，近年も新しいアイデアの導入が数多くなされている．M. Thorup はダイナミックアルゴリズムの設計指針についての最新の成果を紹介した．まず最小全域木についての議論でアイデアを示し特に最近話題になっているダイナミックな最短路問い合わせ構造についての解説を行った．　また，U. Zwick は，近似的な最短路問い合わせ構造であるスパナーに関して，加法的な誤差を考慮した設計を紹介した．さらに，J. Diaz はメッシュ上を移動する複数の通信体の形成するアドホックネットワークの連結度などの性質の確率的解析について講演を行った．

計算複雑度理論に関する最近の進展

計算理論の中核である計算複雑度理論では 3 つの講演があった．U. Feige は NP 完全問題に対するヒューリスティクスの理論解析として，通常の平均解析よりも実用的なモデルの模索について様々なアプローチを紹介し，特に 3SAT 問題において実用的に高速なヒューリスティクスの（現実的な意味で平均的な）効率性に対する解析法を解説した．渡辺治は 3CNF-SAT において，解の近傍にあるアサインメントが与えられた時の局所探索アルゴリズムでの求解の解析と実験結果を示した．さらに，L. Fortnow は，彼の選んだ最近十年での計算複雑度理論の成果 10 件とその意義を的確な描写で述べ, それ以前の十年の 10 件の成果との比較や進展の模様を示した．戸田，渡辺，荻原といった日本人研究者の成果も含まれており，興味深いものであった．

Short talks

8 件の Short Talk はグラフアルゴリズム，WEB 解析，計算幾何学，ワイアレスネットワークの解析，分散アルゴリズム，計算経済学など多様なテー

マであり，上原隆平（JAIST)，陳致中（東京電機大学），増山繁（豊橋技術科学大学），小野廣隆（九州大学)，定兼邦彦（九州大学)，浅野泰仁（東北大学），浅野哲夫（JAIST），塩浦昭義（東北大学）というプロジェクトのメンバーである第一線研究者が講演し，どれも多くの聴衆を集めた．

4　総括と今後

ビジネスミーティングにおいては，本特定領域研究メンバーと外国人招待講演者たちを交えた活発な討議がなされ，アメリカ, ヨーロッパなどでのプロジェクトの活動例の紹介，今後の協力体制への意見，学生交換の提案などがなされた．本国際会議に関しては非常に優れた催しであるという評価を受け，継続して同様な研究交流の場を持つ事が多くの参加者から希望された．更にチュートリアルやサマースクールなどを含めた多くの提案がなされた．具体的な企画に関しては総括班で検討を行っている．

電子情報通信学会 2005 年総合大会チュートリアル講演
「計算限界の中心で解法を叫ぶ」

担当者:　山下雅史 (九州大学), 牧野和久 (大阪大学)

計算機科学分野における理論と応用の乖離が指摘されて久しい．この乖離を埋めるための方策の一つとして, 広く応用に携わる方との話し合いの場を設定することを目的として, 電子情報通信学会コンピュテーション研究会と共催でこのチュートリアル講演を企画・実施した．プログラムの詳細は以下に示しているが，2 部構成を取り，第 1 部は応用分野に現れる具体的な問題を理論的に検討する場合に生ずる様々な問題について 4 名の方に御講演を頂き，第 2 部では，更に 2 名の方にも加わって頂き，計 6 名の方にブースを設定して頂いた上で，問題相談コーナーを実施した．第 1 部は立ち見が出る程の盛況で 70 名を超える聴衆に集まって頂き，改めて「理論と応用の乖離を埋める」ことに対する研究者の要請が強いことを感じた．第 2 部は始めての経験ということもあり，30 名程度の参加があったが，具体的な問題の相談件数は期待された程ではなく，検討の余地を残した．

プログラム

日時:

平成 17 年 3 月 23 日 (水曜) 13 時〜17 時

会場:

大阪大学 豊中キャンパス ロ号館 308, 309 教室

第 1 部: 講演

司会: 山下 雅史 (九州大学)

杉原 厚吉 (東京大学) 「幾何計算駆け込み寺住職体験記」

徳山 豪 (東北大学) 「計算理論の先端的手法による実用分野開拓– データマイニングを例にして」

玉木 久夫 (明治大学) 「組合せ最適化に対する巨大近傍アプローチ」

柳浦 睦憲 (京都大学) 「メタヒューリスティックスに基づく問題解決エンジン」

第 2 部: 問題相談コーナー

第 1 ブース: 杉原 厚吉 (東京大学)

第 2 ブース: 徳山 豪 (東北大学)

第 3 ブース: 玉木 久夫 (明治大学)

第 4 ブース: 柳浦 睦憲 (京都大学)

第 5 ブース: 渡辺 治 (東京工業大学)

第 6 ブース: 定兼 邦彦 (九州大学)

第18回 回路とシステム軽井沢ワークショップ講演企画

担当者:　巳波弘佳 (関西学院大学)

本特定領域研究の活動の広報と他分野の研究者との交流を目的に，電子情報通信学会 回路とシステム軽井沢ワークショップに招待講演セッションを企画した．

本ワークショップは，回路とシステムに関連した分野の研究者や技術者が集い，招待論文や投稿論文，パネル討論を通じて，分野内だけでなく分野間にまたがる境界領域の課題解決と，将来の研究分野の探求を目的として開催されているものである．この分野の研究集会としては国内で最大規模であり，また今回で 18 回目となり，定評のあるワークショップである．大学の研究者のみならず，企業研究所からの参加も数多く，産学の交流も盛んである．

このワークショップは，回路とシステム関連分野としてアルゴリズム関係，グラフ理論関係の講演も行われているため，関心を持つ聴衆も多く，ここで今回のセッションを企画することは有効だと考えられる．

以下に，関連プログラムを挙げる．

第18回 回路とシステム軽井沢ワークショップ

【日程】 2005 年 4 月 25 日 (月), 26 日 (火)

【場所】 軽井沢プリンスホテル・西館・国際会議場

【URL】 http://www.ieice.or.jp/ess/kws/

本特定領域研究関連セッション

セッション D2-1 (4/26 9:30-10:15)
動きだした特定領域研究『新世代の計算限界』(1)

- 「プロジェクトの概要 ―計算限界の過去・現在・未来―」伊藤大雄 (京大)

セッション D2-2 (4/26 10:30-12:00)
動きだした特定領域研究『新世代の計算限界』(2)

- 「オンライン予測の理論と応用」瀧本英二 (東北大)
- 「Witt 分解を用いたフーリエ解析 ― MOD 回路サイズの下限証明のための新しい代数―」築地立家 (東京電機大)

研究集会の計画：特定領域「確率的情報処理」との共同開催

ランダムネスと計算
Randomness and Computation

幹事：田中 和之，徳山 豪（東北大学），渡辺 治（東京工業大学）

1　経緯と趣旨

ランダムネス（ランダム性やランダムリソースなどの総称）は，多くの現象に現われるが，情報処理や計算にも，様々な形でかかわってきている．計算が扱う対象の中に含まれるランダムネスはもちろんのこと，ランダムネスを計算の効率化に積極的に応用しよう，という考えかたも，最近のアルゴリズム設計の基本方針の一つになりつつある．

情報処理や計算に関わるランダムネスの研究には，計算機科学，情報科学，さらには統計物理学など，異なる分野の研究者が，それぞれ，独自のアプローチで取り組んでいる．そのような中で，計算と情報処理に関する二つの科研費特定領域—新世代の計算限界，確率的情報処理 — が，ランダムネスと計算に関し，両領域で行なわれている最先端の研究を紹介するワークショップを共同開催し，同じような研究をしている多くの研究者に，意見交換の場，そして，さらには新たな交流の場を提供することを計画した．

2　日程とプログラム案

会議は４日間の予定で，その中で，二特定領域の研究者により，ランダムネスと計算に関する研究成果の発表を約 30 件行う予定である．また，チュートリアル講演を 4 件予定しており（それぞれの領域から 2 件を推薦），最新の解析技術やアルゴリズムの考え方を取り上げ講演してもらう予定である．なお，チュートリアル講演後には，招待講演者とポスターセッション風に質疑できる場を設けるなど，分野外の研究者でも理解できるような工夫を計画している．

具体的には，以下のような計画で準備を進めている．

名称： ランダムネスと計算
Randomness and Computation)
月日：２００５年7月１８日〜２２日
場所： 仙台国際センター
形態： チュートリアル講演と関連研究の発表
公開，参加費無料

チュートリアル講演予定者
Ravi Kannan (Yale University)
松井 知己（東京大学，情報理工学系研究科）
福島 孝治（東京大学，総合文科研究科）
田中 和之（東北大学，情報科学研究科）

その他の詳細や一般の発表予定者，講演題目などは，下記のウェブページを参照．

http://www.smapip.is.tohoku.ac.jp/~smapip/2005/NHC+SMAPIP/

ミニ研究集会 (研究の種をいかに育てるか)

世話役: 浅野 哲夫，上原 隆平，元木 光雄
(北陸先端科学技術大学院大学)

日時　3月 12 日 (土)
午前１０時から午後５時

場所　北陸先端科学技術大学院大学
情報科学研究科，コラボレーションルーム

目的　従来，日本の大学では講座以外の研究者とは共同研究を行わないという講座制の悪い側面に縛られていた傾向があった．特定領域研究「新世代の計算限界—その解明と打破」においては，研究のスタイルについても講座，大学の枠を超えて研究者が共同して研究を行うという新たな流れを作ることを目標の一つに掲げている．このミニ集会もその趣旨に沿ったものである．つまり，特定のテーマを決めるのではなく，参加者が持ち寄った問題を互いに披露することから始めて，如何にして違った視点で研究の種を育てるかに目標を置く．したがって，完成された研究テーマよりも，むしろまだ研究の対象として成り立つかどうかが分からない話題を参加者が持ち寄って，異なる視点から新たな可能性を探ることが重要である．

参加者　浅野 哲夫，上原 隆平，元木 光雄
（北陸先端科学技術大学院大学 情報科学研究科）
渡辺 治（東京工業大学 情報理工学研究科）
堀山 貴史（京都大学大学院 情報科学研究科）
宇野 毅明，清美 礼（国立情報学研究所）

議論の内容　午前中は東工大の渡辺が集合の分割問題を取り上げた．一般には困難なこの分割問題は，データマイニング等の応用がある．そして現実的には propagation search と呼ばれる手法が有効であり，実際に幅広く用いられている．しかし，この propagation search がなぜ多くの場合に有用なのか，理論的な解析はこれまでほとんど行われていない．そこで渡辺がこの手法の理論的なふるまいに関する問題提起を行い，議論を行ったが，やはり詳細な資料が必要だ，という結論に達した．この問題については，渡辺から参加者に後日資料を送付した後で議論を再開することとした．午後には，上原がインターバルグラフにおいて最長路を求める問題を提起し，午後のすべての時間を使って議論を行った．まず，上原が現在までの状況を詳しく説明した後，最長路を求めるためのラフなアイディアを披露した後，どこに難しさがあるか，関連する研究成果は何かを説明した．具体的な例題に即した議論の後で，ハミルトン路問題と密接な関連があることが分かり，始点だけを指定した場合，始点と終点を任意に指定した場合のハミルトン路の発見問題を考察した．ダブルスタック法と我々が名づけた方法を発見し，その正しさもほぼ証明できたのではないか，という所で１日の議論を終えた．

１日だけの議論でもちろん論文になるだけの研究成果は得られなかったが，今後この議論をメールを交換しながら継続することもできるので，いつか成果につながるのではないかと期待できる．今回集まった人数は全体でも７名と少なかったが，逆に一つのトピックに絞って議論をするには適当な人数であった．特に興味深かったのは，目の付け所が各人で異なり，なるほどそんな考え方をするのかと感心させられたことが多かった．ドイツには，このような議論ベースの集会をサポートする施設（ダグシュツール）があり，世界各国から毎週研究者が集まって共同研究を行っている．日本では他大学に属する他人と議論して共同で論文を執筆するという機会がまだ少ない．この研究集会では完成された論文を解説するのではなく，どのようにして問題提起から論文の形にまとめていくのかというプロセスが「見える」ので，学生にとっては研究の進め方を学ばせる意味で最適であると言える．今後も，次代を担う若手研究者育成のためにも，このようなミニ集会を頻繁に開いていきたい．

ミニ研究集会 (グラフアルゴリズム)

世話役: 田中圭介 (東京工業大学)，戸田誠之助 (日本大学)

Chordal graph に関する計算問題ならびにアルゴリズムを中心に，研究成果の発表と新たな課題探求に向けた討論を行った．詳細は次の通り．

日時： 3 月 19 日 (土)　午前 10 時 ~ 午後 6 時
場所： 日本大学文理学部 8 号館レクチャーホール
参加者数： 19 名
研究発表：

(1) 10:00~11:20，Computing automorphism groups of chordal graphs whose simplicial components are of small size，戸田誠之助（日大文理）
（概要）小さなサイズの単体成分へと分解可能な任意の chordal graph に対して，その自己同型群が多項式時間計算可能であることを示した．

(2) 11:30~12:30，2-リンクパズルの多項式時間解法，牧野 格三（東工大）
（概要）ナンバーリンクパズルを「k-リンクパズル」と呼ばれるグラフ論的な計算問題へと一般化し，3 × (偶数) や 4 × (偶数) といった格子グラフに関する 2-リンクパズルに対して多項式時間アルゴリズムを示すとともに，一般の格子グラフに関する予想を述べた．さらに，参加者を交えた討論を経て新たな研究課題が見出された．

(3) 13:30~15:00，On the Laminar Structure of Ptolemaic and Distance Hereditary Graphs，上原 隆平 (JAIST)，宇野裕之 (大阪府立大学)
（概要）Chordal graph（のクラス）と distance hereditary graph（のクラス）の共通部分として特徴付けられている Ptolemaic graph（のクラス）に対して，ある種の木表現モデルが存在すること，その木表現モデルが各 Ptolemaic graph に対して一意的に定まること，ならびに，その木表現モデルを線形時間で構築できることを示した．さらに，この結果をもとに，Ptolemaic graph（のクラス）に対する認識問題や同型性判定問題が線形時間計算可能であることを示した．また，この研究の発展的可能性として，distance hereditary graph に対する同様の木表現モデルの存在性に関する予想を述べた．

(4) 15:15~16:45，On precoloring extension problem，名古屋孝幸（東京電機大学）
（概要）グラフの precoloring extension problem (PREXT と略す) に対して，一般のグラフに対しては NP 完全であることや，クリーク数を制限した chordal graph に対して多項式時間計算可能であることを紹介した．また，PREXT を制限した 1-PREXT 問題に対して，chordal graph に対するネットワークフローを用いた多項式時間アルゴリズムを紹介した．

研究発表終了後，午後 6 時頃まで討論を行った．討論の間に，グラフ自己同型群問題の応用研究として，河内亮周氏（東工大）に次の成果を発表して頂いた．

(5) Computational Distinguishability between Quantum States and Its Applications，A. Kawachi, T. Koshiba, H. Nishimura and T. Yamakami
（概要）確率分布に対する判別問題の自然な一般化として，二つの量子状態を判別する問題（QSCDff）を新たに定義し，その問題が落とし戸関数の性質を有すること，その最悪計算量と平均計算量が等価であること，さらに，その最悪計算量がグラフ自己同型群問題の最悪計算量と同等以上であることを示した．

各地から多くの参加者を得て活発な討論が行われ，発展的研究課題を見出すこともできて，とても充実した研究集会であった．

ミニ研究集会 (量子計算)

世話役: 西野 哲朗 (電気通信大学)

２００５年3月２６日（土）１３：００ より，電気通信大学総合研究棟８階８０７セミナー室で，量子計算に関するミニ研究集会を開催致しました．当日は，まず最初に，國廣昇先生（電気通信大学情報通信工学科）による,「近似を導入した加算剰余演算の成功確率の評価」という題目の講演が行なわれました [1]．その後に，参加者全員によるフリーディスカッションを行いました．講演は１６時頃に終了し，その後，１８時頃まで，ディスカッションを行いました．

まず，講演では，近似を導入した加算剰余演算の成功確率について解説されました．Draper が提案した量子加算を構成要素として加算剰余を構成する場合，その大部分の計算時間は，付加的に加えられた量子フーリエ変換部であることが知られています．この問題に対して，近似量子フーリエ変換を導入することにより，計算時間が削減できると，Draper や，Beauregard により，主張されています．しかしながら，彼らは，厳密に評価を行なっているわけではないそうです．そこで，本発表では，近似精度と加算剰余演算の成功確率に関して，厳密な評価が提示されました．この評価を用いることにより，加算剰余演算を構成要素として，Shor のアルゴリズムを構成した場合の，素因数分解の成功確率の評価を行なうことが可能となります．

当日の参加者は，講演者の國廣先生の他，特定領域Ｂ０４グループからは，垂井先生と西野が参加し，さらに，電通大大学院の博士課程の学生が１名参加しました．また，本ミニ研究集会の告知をご覧になった（株）日立製作所システム開発研究所の２名の研究員の方も参加されました．年度末ということもあり，この６名でこじんまりと議論を行いましたが，逆に，このくらいの規模ですと，フランクに質問ができますので，講演の最中も，盛んに質問が出され，終始，インタラクティブな雰囲気の研究集会となりました．

講演の本題に入る前には，現在のコンピュータでは，因数分解はどのくらい高速に行なえるのか? もし，因数分解を行なう量子コンピュータが実現できるとしても，そのために莫大な資金が必要だとしたら，その資金を出す機関は世界の何処にあるのか？などの，一般的な話題についても，議論がありました．

一方，講演後のフリーデスカッションは，まさに，自由な討論会となりました．

まず，現在，プリンストン高等研究所に在籍する S. Aaronson が，彼の博士学位論文の中で述べた，Shor のアルゴリズムの物理的実現可能性に関する懐疑論 [2] について議論が行なわれました．また，その同じ Aaronson が，最近研究している，アナログ的な計算装置による NP 完全問題の高速解法の可能性についても，若干，議論になりました．

そうした話の流れを受けて，さらには，P = NP ? 問題解決に向けての展望についても，意見が交換されました．例えば，最新の計算量理論の成果を勉強すると，P = BPP が信じられるようになってくるとか，P = NP ? 問題を直接考えるよりは，NP = coNP ? 問題を考えた方が良いのではないか，といった意見などが出されました．

参考文献

[1] N. Kunihiro, “Exact Analyses of Computational Time for Factoring in Quantum Computers ”, *IEICE Transactions on Fundamentals*, Vol.E88-A, No.1, pp.105–111 (2005).

[2] S. Aaronson, “Multilinear Formulas and Skepticism of Quantum Computing ”, to appear in *SIAM Journal of Computing* (Also in *STOC 2004*, pp. 118-127, and quant-ph/0311039).

ミニ研究集会 (論理関数)

世話役:　宮崎 修一, 堀山 貴史 (京都大学)

開催日時： 2005 年 3 月 28 日 (月)　10 時 30 分〜17 時

開催場所： 九州工業大学　天神サテライトキャンパス　(福岡市中央区天神 1 丁目 7 番 11 号 イムズ 11F)

参加者： 朝廣雄一（九州産業大学），小野廣隆（九州大学），黒田太陽（九州工業大学），定兼邦彦（九州大学），玉置卓（京都大学），原口和也（京都大学），堀山貴史（京都大学），牧野和久（大阪大学），宮崎修一（京都大学），宮野英次（九州工業大学），森住大樹（京都大学），山下雅史（九州大学）

1　はじめに

本研究集会は，各参加者が現在取り組んでいる問題や既に発表した成果について，紹介やディスカッションを行うことにより，研究の進展を図ろうという目的で開催された．論理関数をメインテーマとしているが，その他，本特定領域研究に関わる話題ならば広く対象とした．各人が 1 つずつテーマを用意して来たようであったが，時間の都合上，以下の 5 件について話題が提供された．

2　決定木のサイズの平均値について (10:30〜12:00)

原口和也氏より，現在取り組んでいる問題が紹介された．n 変数論理関数 f を表現する頂点数最小の二分決定木の頂点数を f のサイズと定義する．n 変数関数全体のサイズの平均値はいくらになるかというのが問題であった．$n^{\log n}$ 下限の議論が原口氏から説明され，その証明が正しいであろうことが参加者の間で確認されたが，実際の値は 2^n であろうというのが，大方の予想であった．また，決定木が定数割合エラーを許して良いという緩和の下で，どの程度サイズを減らすことができるかについても議論された．

3　3SAT に対するアルゴリズムの計算時間の上限 (13:00〜14:30)

玉置卓氏より，研究成果の紹介がなされた．3SAT に対する確率アルゴリズムの計算時間の上限は，1999 年に Schöing によって発表された 1.334^n が最良であったが，それを 1.324^n へと改良した．そのアイデアは以下の通りである．Schöing のアルゴリズムで解が多い場合の計算時間を解析し，解の数が多いほど高速になることを示した．また，PPSZ というアルゴリズムは，逆に解が少ないほど高速になる．これらを同時に走らせることにより，互いの欠点を補い，高速化できることを示した．

SAT は直感的には解の数が多いほど易しいが，PPSZ の計算時間解析はその逆である．この現象は解析の都合上によるものが大きいと見られており，実際には PPSZ も解が唯一である場合の計算時間が最悪であろうことが予想できる．この直感を証明することができれば，上限の大幅な改良が可能となる．

4　回路計算量の下限　(14:30〜16:00)

森住大樹氏より，研究成果が報告された．ここでは，AND, OR, NOT のみを使用する論理回路を考える．論理回路 C のサイズとは，C に含まれる AND 素子の数と OR 素子の数の和である．論理関数 f の回路計算量とは，f を計算する最小サイズの論理回路のサイズである．これまで具体的な関数で最良の下限は，Lachish と Raz による $4.5n - o(n)$ であったが，それを $5n - o(n)$ へと改

良した．Lachish と Raz の下限は，Strongly-two-dependent な関数に対して入力を削除していく手法を用いていたが，その場合分けを細かく解析することにより，下限の改良を成功させた．

5 Right-hand-on-the-wall walk (16:00〜16:30)

定兼邦彦氏より，研究成果が報告された．与えられたグラフの各頂点 v（次数を $d(v)$ とする）に対して，その接続枝に番号を 1 から $d(v)$ まで重複なく割り当てる（枝 (u, v) に対して，u から見た番号と v から見た番号は異なって良い）．このとき，以下の条件を満たす番号割り当てができるかどうかという問題を考える．(以下では，頂点 v から見て番号 k が付けられた枝を v_k と書く.)

条件： 枝 1_1 から出発し，グラフの枝を辿り，全ての頂点を訪れて頂点 1 に戻る．ただし，頂点 v に枝 v_k から入ってきた場合は，枝 v_{k+1} から出ていく．

任意のグラフに対して，この条件を満たす番号割り当てが存在し，その閉路の長さは高々$10n$ であることが，この研究で明らかにされた．また，閉路長を $4n$ よりも短くすることができないグラフの存在も示された．このギャップを埋めることは興味深い未解決問題であるが，定兼氏の予想は $4n$ である．

6 無線ネットワークにおける通信電力量に対するオンラインアルゴリズム (16:30〜17:00)

小野廣隆氏より，研究成果の紹介があった．1 台のサーバと複数のクライアントが無線で通信する状況を考える．サーバは n 台のクライアントと通信を行いたいが，クライアントがどの位置にいるかを知らないため，どの程度の電力で発信すれば良いかが分からない．例えば，多くのクライアントに一度に届くように大きな電力量で発信すると，多くのクライアントが近くにいた場合の損が大きい．逆に少しずつ到達エリアを拡大しながら（つまり電力量を大きくしながら）繰り返し送信すると，遠い場所にクライアントがいる場合に，何度も送信しなければならないので損失が大きい．ここでは，送信したいクライアント数に応じたある割合でエリアを広げながら送るアルゴリズムの競合比 $3/2 + \sqrt{2}$ を示し，そのアルゴリズムが最適であることも示した．

ミニ研究集会 (列挙アルゴリズム)

世話役:　宇野 毅明 (情報学研究所), 中野 眞一 (群馬大学)

本研究集会は，最近の列挙アルゴリズム研究に関する情報交換と議論を行うセミナーである．列挙アルゴリズムは科学・産業のさまざまな場面で使われているが，その使用頻度の高さに比べ，アルゴリズム理論からの研究は立ち遅れている．本セミナーは，理論的な全身と現実問題への適用の両面から，列挙アルゴリズム，および列挙に関連する組合せアルゴリズムに関する議論を行い，列挙アルゴリズムの研究を推し進めるものである．

日程: 2005 年 3 月 29 日〜3 月 31 日
場所: 群馬大学伊香保研修所
参加メンバー:
宇野 毅明 (国立情報学研究所)
中野眞一 (群馬大学)
菊地 洋右 (ERATO)
堀山貴史 (京都大学)
上原 隆平 (北陸先端科学技術大学院大学)
松井泰子 (東海大学)
宇野裕之 (大阪府立大学)
田中勇樹 (群馬大学)
河合博之 (群馬大学)
山崎浩一 (群馬大学)
元木光雄 (北陸先端科学技術大学院大学)
川野晋一郎 (群馬大学)
山中克久 (群馬大学)
蓮沼徹 (徳島大学)
荒木徹 (岩手大学)
清見礼 (国立情報学研究所)
長井歩 (群馬大学)
岡本吉央 (スイス連邦工科大学)
宮本裕一郎 (上智大学)
David Avis (McGill University)

当日は，以下のような発表と議論が行われた．

1. 方形描画グラフの圧縮について
　山中克久 (群馬大学)
2. ラベル付コーダルグラフの列挙法
　清見礼 (国立情報学研究所)
3. 航空経路決定問題について
　上原隆平 (北陸先端科学技術大学院大学)
4. 2 分木の列挙について
　川野晋一郎 (群馬大学)
5. k 分木の isoperiodic number について
　山崎浩一 (群馬大学)
6. linear code の列挙について
　菊地 洋右 (ERATO)
7. Larman graph の列挙について
　David Avis (McGill University)
8. フリーディスカッション

グラフの圧縮は，列挙したグラフを効率良くメモリに格納するために必要な技術である．ここでは，多数のグラフが存在した場合に，相互の差分を用いてより小さな領域で記憶できないか，という議論が出た．

コーダルグラフの列挙，2 分木の列挙では，問題の紹介，効率の良いアルゴリズム，数え上げへの応用といった解説があった．また，今後，インターバルグラフや順序木へと発展させたらどうかといった意見があった．

航空空路決定問題では，空港の利用客数から最適な航空経路を決定する問題に対して，ある種のシンプルなモデルと多項式時間の解法が紹介された．利用客の行き先を含んだモデルについても議論を行ったが，今後の課題となった．

フリーディスカッションでは，グラフ圧縮ででた疑問点に関する解答や，いくつかの発表で現れた web グラフに関する解説や議論などが行われた．

全体を通して，非常に活発に議論が行れ，各人の研究結果や問題に関して，より新しいモデルや問題，お互いの疑問点に対する情報やアイディアの提供，といった研究者間のコミュニケーションにおいて重要なことがらが多く行われた．このセミナーは参加者の研究を進める大きな力となるであろう．

2.　研究課題別活動報告

A01: オンライン予測の手法を用いた意思決定モデルに関する研究

瀧本 英二 † 酒井 義文 ‡ 天野 一幸 †

† 東北大学 大学院 情報科学研究科
〒 980-8579 仙台市青葉区荒巻字青葉 6-6-05
{t2,ama}@ecei.tohoku.ac.jp

‡ 東北大学 大学院 農学研究科
〒 981-8555 仙台市青葉区堤通雨宮町 1-1
sakai@biochem.tohoku.ac.jp

1 はじめに

意思決定とデータの提示が交互に繰り返されるオンラインでの意思決定過程に関する問題は，機械学習，情報圧縮，言語モデル，ゲーム理論，ファイナンス，ルーティングなど様々な分野に現れる普遍的なものである．また，インターネットやゲノム解析などの急速な発展に伴い，膨大なデータが逐次的に与えられる状況のもとで解決しなければならない新しい問題が次々と提起されている．本研究では，これらの問題を統一して扱うことのできる普遍的なモデルの構築，および，様々な評価基準のもとで理論的に保証された性能を持つ意思決定手法の設計と解析手法の確立を目指し，次に述べる３つのアプローチを試みている．

１つめは，計算学習理論の分野で開発されたオンライン予測の手法を手がかりにしようとするものである．この観点から，今年度は以下の成果を得た（２章）．従来の動的資源分散モデルを拡張し，投資の対象となるオプションの損失の範囲（リスク情報）がオプションごとに異なり，それらが予め知らされている場合について，統合アルゴリズムの設計と解析を行い，厳密な性能評価を与えた．また，複数の仮説を統合して予測性能の良い仮説を構築するブースティングの問題に対し，サンプルの分割と併合を繰り返すことによって決定ダイアグラムを構成する新しいスキームを得た．これは，従来異なる原理に基づくものと思われていた AdaBoost タイプと決定木生成タイプのブースティング手法を統一的に扱うための理論的枠組みを与えるものである．

２つめは，さまざまな分野の問題で，社会的・学術的に求められている品質保証を明らかにし，本研究に還元しようとするものである．この観点から，今年度は，ネット上の文書の検索問題に着目し以下の成果を得た（３章）．ネット上の新規文書の公開及び既公開文書の改訂を即時に認識し，ユーザへの検索結果に直ちに反映させることのできる検索システムの構築を目指して，互いに協調する複数個のサーバによって構成される分散型の検索エンジンの開発を進めた．特に，アーキテクチャの観点からの対故障性の向上に関する技術を提案し，その有効性を検証した．また，検索結果の提示法として，公開や改訂の時刻に依存した文書の新しさを加味した文書採点法を提案した．

３つめは，意思決定アルゴリズムが保持すべき表現の複雑さに注目し，アルゴリズムの計算量的な限界について考察しようとするものである．この観点から，今年度は論理関数の複雑さに注目し以下の成果を得た（４章）．二次関数の積素子計算量について，単層回路と複層の回路において指数関数的なギャップの生じる場合があること，および，このギャップの上界が２階の指数関数で抑えられることを示した．また，乗算を行う従来より小さいサイズの順序付き二部決定グラフ（OBDD）を設計した．さらに，しきい値素子を用いた回路において，重みに制限をおかない１層のしきい値回路を，多項式的重みを持つ２層のしきい値回路によって模倣する，従来よりも効率の良い手法を与えた．

2 オンライン予測とブースティング

計算学習理論の分野で開発されたオンライン予測のモデルで最も適用範囲の広いものに，資源の動的配分問題があり，次のように定式化される．

投資の対象（オプション）が K 個あるとし，投資の方法についてアドバイスを行う「エキスパート」が N 人いると仮定する．各時刻 $t = 1, 2, \ldots$ において，各エキスパート i は，投資ベクトル $x_{i,t} = (x_{i,t}(1), \ldots, x_{i,t}(K))$ を提示する．ただし，投資ベクトルは確率ベクトル，すなわち，各成分が非負で成分の総和が 1 であるとする．これらを受け，投資アルゴリズム（学習者と呼ぶ）は，自分の投資ベクトル $p_t = (p_t(1), \ldots, p_t(K))$ を定める．その後，各オプション j のコスト $l_t(j) \in [0, 1]$ が明らかとなる．このとき，学習者は，投資ベクトルとコストベクトルの内積 $p_t \cdot l_t = \sum_{j=1}^{K} p_t(j) l_t(j)$ の損失を被る．同様に，各エキスパート i も損失 $x_{i,t} \cdot l_t$ を被る．学習者の目標は，このプロセスをある時刻 T まで行った後の累積損失 $\sum_{t=1}^{T} p_t \cdot l_t$ を，最適なエキスパートの累積損失 $\min_i \sum_{t=1}^{T} x_{i,t} \cdot l_t$ に比べてそれほど大きくならないようにすることである．この問題に対し，ヘッジアルゴリズムと呼ばれる単純な重みつき平均アルゴリズムが，ほぼ最適な性能を与えることが知られている．

本研究では，各オプション j のコスト $l_t(j)$ がいずれも一様に 1 で上から抑えられているという仮定を緩め，その上界（リスク情報）b_j が予め与えられているというモデルを提案した．リスク情報は，競馬の投資におけるオッズ情報に対応するものであり，非常に自然な概念である．このモデルの下で，Vovk の統合アルゴリズム（Aggregating Algorithm）を詳細に解析し，その性能の厳密な評価を与えた．その結果，リスク情報に大きな偏りがある場合，ある一定値以下のリスク情報は，アルゴリズムの性能に影響を与えないという意外な性質が明らかとなった．

また，精度の低い複数の仮説を統合して予測精度の高い仮説を構築するブースティングの問題に対し，一つの新しい設計手法を与えた．ブースティングは，動的資源配分問題の双対問題という見方もできることが知られており，オンライン予測とは非常に関連が深い問題である．

ブースティングは，以下のような共通のスキームの元で論じることができる．サンプル $\{(x_1, y_1), \ldots, (x_m, y_m)\} \subseteq X \times \{-1, 1\}$ が与えられていると仮定する．ここで，X は適当なインスタンス空間である．各時刻 $t = 1, 2, \ldots$ に対し，ブースターはサンプル上の分布 D_t を作り，分布 D_t のもとでのマージンの期待値が正の仮説（弱仮説）$h_t : X \to \{-1, 1\}$ を得る．すなわち，$\sum_{i=1}^{m} D_t(i) h_t(x_i) y_i > 0$．ある時刻 T において，ブースターは弱仮説 $h_1, \ldots, h_T$ を統合してマージンの最小値が正の仮説 F_T を構成する．すなわち，任意の i に対し，$F_T(x_i) y_i > 0$.

ブースティングには大きく 2 通りの設計手法が知られている．一つは，マージン空間上にポテンシャル関数 ϕ を導入し，$\sum_i \phi(F_T(x_i) y_i)$ が最小となることを目指すもので，AdaBoost，InfoBoost，LogitBoost などがこの設計手法に基づくものである．もう一つは，ラベル空間の分布上にエントロピー関数を導入し，結合仮説の与える条件付エントロピー $H(Y|F_T)$ が最小となることを目指すものである．C4.5 などのトップダウン型決定木生成アルゴリズムや，これを改良して決定ダイアグラムを生成する MM アルゴリズムなどがこの設計手法に基づく．

従来，これらの 2 つの方法論はまったく異なるものだと思われていたが，本研究では InfoBoost がある意味で決定ダイアグラムを生成していることに注目し，これを一般化することによって，これら 2 つの方法論を統一的に論じることのできる新しい設計手法を開発した．すなわち，本研究で得られたブースティング手法は，AdaBoost が用いているポテンシャル関数 $\phi(x) = \exp(-x)$ に基づくタイプ 1 のブースティングアルゴリズムという見方もできるし，MM が用いているエントロピー関数 $G(p_1, p_2) = 2\sqrt{p_1 p_2}$ に基づくタイプ 2 のブースティングアルゴリズムという見方もできる．従って，本研究の成果は，ブースティングの設計手法に対し，統一的な理論的枠組みを与えたいうことができる．

3 文書検索

ネットワーク上の新規文書の公開及び既公開文書の改訂を即時に認識し，ユーザへの検索結果に直ちに反映させることのできる検索システムの設計及び構築を目指して，互いに協調する複数個のサーバによって構成される分散型の検索エンジン CSE(Cooperative Search Engine) の開発を進めており，アーキテクチャの観点からの対故障性の向上に関する技術を提案し，その有効性を検証し

た．また，検索結果の提示法として，公開や改訂の時刻に依存した文書の新しさを加味した文書採点法を提案した．

CSE の概要は以下の通りである．CSE は，ネットワーク上の各局所サーバに存在する局所検索エンジン LSE(Local Search Engine) と，ユーザからの検索要求に応じて適切な LSE に局所検索を依頼する位置サーバ LS(Location Server) からなる．

LSE は，周期的に自身が存在する局所サーバ L おいて新規に公開された文書及び改訂された既公開文書を検知し，L がもつ文書を局所検索する際に用いる索引を更新する．集中型の検索エンジンでは，他の局所サーバにおいて公開されている文書をロボットによって収集した後に索引を更新しなければならないため，新規文書や改訂された文書の内容を短い間隔で索引に反映させることは難しい．これに対して，LSE は L に存在する文書のみを対象とするため，短い周期で頻繁に索引を更新することが可能である．また， LSE は，索引の更新の後に，索引に現れるすべての語を，L 内においてその語が現れる任意の文書に対する最大のスコアとともに LS に送信する．これをメタ索引という．メタ索引は，ユーザからの検索要求の際に，LS が局所検索を依頼する LSE の個数を絞り込む目的で用いられる．更に，LSE は LS からの局所検索の依頼に応じて，L に存在する文書を検索し，結果を LS に返す．

LS は，キーワードをそれが文書中に現れるか否かを表す論理変数にみたてた論理式の形でユーザから指定される検索クエリに対して，各 LSE から送信された索引に存在する語に関する情報を利用することによって，局所検索をする LSE の個数を絞り込む．たとえば，一つのキーワードのみからなる検索クエリが与えられた場合に，そのキーワードが索引に現れない LSE には検索対象となる文書が局所サーバに存在しない．したがって，そのキーワードが索引に現れる LSE のみに局所検索の依頼をすれば十分である．検索クエリが一般の論理式 f である場合も，$f \leq g$ であるような単調な論理式 g を求め，g に現れるキーワードを，それが文書に現れるか否かを表す論理変数とみなすのではなく，それが LSE の索引に現れるか否かを表す論理変数とみなすことによって，$g = 0$ である LSE の局所サーバに $f = 1$ である文書が存在しないことが保証される．ただし，f から最小の g を求めるのは NP 困難であるため，実際には最小な g ではなく，これを近似する単調論理式を用いて，局所検索を依頼する LSE の個数を絞り込む．また，検索結果としてスコアの高い順に n 個の文書を検索するような場合に，OR 演算のみの論理式が検索クエリとして与えられるならば，キーワードを含む文書の最大のスコアに関する情報を用いることで，局所検索を依頼する LSE の個数を高々n に絞り込むことができる．LS は，ユーザからの検索クエリに対して，選ばれた LSE に局所検索を依頼し，各 LSE から返された結果を統合したものを検索結果としてユーザに出力する．

一般に，分散型の検索エンジンは，検索時にサーバ間の通信が生じるため，集中型の検索エンジンと比較して，検索結果を得るまでに時間がかかる．CSE では，上に述べた LS による局所検索を依頼する LSE の個数の絞り込みのほかに，様々なキャッシュ技術を用いて，検索結果を得るまでの時間の短縮化を実現している．ただし，現状ではインターネット規模のネットワークでの検索エンジンとして用いるのは難しく，たとえば社内イントラナットなどの，100 台以下の局所サーバからなる比較的小規模なネットワークでの利用を想定している．以上が，CSE の概要である．

CSE は複数のサーバからなる分散型の検索エンジンであるものの，1 台の LS が他のすべての LSE に接続し，ユーザからの検索要求に対して必ず LS を用いて検索結果を得る．したがって，LS が故障した場合に，CSE のすべての検索サービスが停止する．そこで，LS を複数台用いて冗長な構成に変更することにより，対故障性の向上を試みた．

複数台の LS による CSE の構成の概要は以下の通りである．各 LS は，LSE から送信されるメタ索引を共有しなければならない．しかし，各 LSE がすべての LS に同じ情報を送信するのは，ネットワーク上のメッセージ数を増加させ，輻輳の原因となる．そこで，各 LSE は最寄の故障していない 1 台の LS にのみメタ索引を送信する．また，メタ索引についても，送信メッセージの大きさを小さく抑えるために，前回の更新時の索引からの差分のみを，前回の更新時刻と今回の更新時刻か

らなるバージョン情報と，送り先である LS のみからなる送信済み LS のリストとともに送信する．メタ索引の差分を受け取った LS は，送信済み LS のリストに隣接する LS をすべて加え，送信済みでない送信可能なすべての LS に，受け取ったメタ索引の差分を転送する．なお，メタ索引の差分を受け取った LS は，もし現在保持しているメタ索引のバージョンと，受け取った差分に付随するバージョンに不整合がある場合に，送り主に差分ではなくメタ索引そのものを送信するように要求する．この状況は，LS が故障から復帰した場合に起こり得る．以上により，故障していないすべての LS によって，LSE のメタ索引が等しく共有される．したがって，すべての LS が故障しない限り，CSE のサービスは停止することなく提供される．

各 LS の故障率に対するシステム全体の停止率をシミュレーションによって調べたところ，LS の台数よりも各 LS に隣接する LS の個数の影響が強いことが確認された．ただし，各 LS に重複なくランダムに選ばれた指定された個数の LS が隣接するネットワークトポロジーを用いた．16 台の LS に対して完全グラフをネットワークトポロジーとして用いた場合においては，各 LS の故障率が 90%であっても，システム全体の停止率は 20%程度であり，実用として許容されるレベルの対故障性を有するシステムを実現できることが確認された．

CSE では，検索における文書の順位付けに，TF·IDF の値に基づくスコアを用いている．ここで，TF は，その文書に現れるキーワードの頻度を表し，IDF は，そのキーワードが現れる文書の頻度の逆数の対数を表す．したがって，検索クエリに複数のキーワードが指定されている場合に，検索対象となる文書全体で希にしか現れないキーワードが数多く現れる文書ほど高いスコアが与えられる．このスコアに基づく順位付けを用いた場合に，公開からの時間経過による新鮮さという意味での文書の価値の劣化は，検索結果に反映されない．そこで，文書に各キーワードが現れてからの経過時間に応じて TF の値を減衰させることによって定義される FTF を用いた，FTF·IDF の値に基づくスコアを提案した．

提案した FTF の定義は以下の通りである．t_i を，文書が公開された後の LSE による i 回目の更新の時刻とする．時刻 t_i における TF，FTF の値をそれぞれ，TF_t，FTF_t とする．このとき，

$$\begin{aligned} \mathrm{FTF}_1 &= \mathrm{TF}_1 \\ \mathrm{FTF}_i &= \mathrm{FTF}_{i-1} \cdot \alpha e^{-(t_i - t_{i-1})} \\ &\quad + (\mathrm{TF}_i - \mathrm{TF}_{i-1}) \end{aligned}$$

である．この定義のもとで，Web 上にて文書を公開している特定のサイトに対して，1 ヶ月にわたり各文書における FTF の値の推移を観察したところ，新しくかつキーワードに関連性の高い文書が上位に順位付けられる傾向が確認された．

CSE を設計する上での今後の重要な課題は，LSE 同士のメタ索引の交換により，各 LSE が LS の部分的な役割を担う仕組みを組み込むことである．時間の経過とともに変化する各局所サーバの文書集合に対して，どの LSE がどの LSE のメタ索引をもつことが検索の高速化につながるかの判断については，オンライン予測の手法が有用となる状況が存在するものと予想される．

4 論理関数の複雑さ

個々の論理関数を，各種の計算モデルを用いて表現する際に必要なサイズを評価する問題，特に，そのサイズに対する下限を求める問題は，計算量理論における挑戦的かつ中心的課題のひとつである．これら表現のサイズは，対応する概念の学習の困難さとも密接に関係することから，学習理論の立場からも基本的研究課題として位置づけられている．

本研究では特に，単調論理回路，しきい値回路，順序付き決定二分木といった，理論上あるいは実用上重要な各計算モデルに対する，種々の論理関数の計算複雑さについて研究を行った．

単調論理回路とは，論理積素子と論理和素子からなる組み合わせ論理回路である．単調論理回路は，論理否定素子を用いることのできる一般の組み合わせ論理回路に比べ，表現できる関数が単調性を有するものに限定されるという制約を受けるものの，実用上現れる多くの関数は，単調性を有しており，それゆえ汎用性の高い回路モデルであるといえる．80 年代半ば，近似法と呼ばれる手法を用いて，明示的に定義された関数を計算する，

単調回路のサイズに対する指数関数的な下界が初めて証明されて以来，単調性の制約を乗り除いた一般の論理回路のサイズに対して強い下界を証明し得る手法の開発が熱望されてきた．しかしながら，入力変数の個数の定数倍を超える下界を示すことすら未だ実現しておらず，この問題は計算の複雑さの研究者にとっての悲願とすらなっている．

本研究では，従来型証明手法の限界点を見極め，これを克服する新手法の開発を目指すことを目的とし，特に，二次関数，すなわち，丁度 2 個の変数の積の論理和として表される関数をとりあげ，論理回路の構造的性質が，この種の関数の計算に要する回路サイズに及ぼす影響について調べた．単調論理回路の層数とは，入力から出力に至る道上における論理積素子の個数の最大値と定義する．また，二次関数の積素子計算量とは，その関数を単調論理回路で計算する際に必要な論理積素子の最小個数と定義する．二次関数は明らかに単層の単調論理回路で計算可能であるが，層数を増加させた場合に，どの程度回路サイズが減少し得るのか等，多くの問題が未解決のまま残されていた．本研究では，二次関数の計算における，単層回路と複層回路を用いたときの計算量や積素子計算量の差について調べ，以下の結果を得た．

まず，二次関数の積素子計算量について，単層回路と複層の回路において指数関数的なギャップの生じる場合があることを明らかにするとと共に，このギャップの上界が 2 階の指数関数で抑えられることを証明した．また，論理和素子と論理積素子の両方を考慮に入れた場合，二次関数を計算する最適な回路は単層回路であることを予想した，いわゆる単層予想と呼ばれる十数年来の未解決問題に対し，多出力関数を考えた場合にはこの予想が偽であることを示し，部分的に解決した．この予想は，その後，Jukna によって単出力関数の場合にも偽であることが証明され，完全な解決を見た．本研究における結果は，本予想解決への足がかりとなる有効なものであったと考えられよう．

順序付き二分決定グラフ (Ordered Binary Decision Diagram，以下 OBDD) は，近年非常に活発に研究されている論理関数の表現形式である．OBDD は，各節に論理変数が割り当てられた決定二分木であり，かつ変数の出現する順序が根から各葉に至る道上で一様であるという制約を満たすものをいう．OBDD は，変数の出現順序を固定した場合には，その表現の最少化や等価性判定が非常に効率良く出来，この性質を利用して VLSI の正当性の検証や，学習に際しての知識表現等の場面で幅広く用いられている．

OBDD は，変数順序を上手く選択することによって，数多くの実用上有用な関数を，非常に効率よく表現することができる一方，基本的かつ重要な幾つかの関数は，いかなる変数順序の元でも，その表現サイズが指数関数的となることが知られている．2 進数で与えられた整数同士の掛け算は，この様な性質を持つ最も代表的な関数である．90 年頃に Bryant によって証明されたこの事実は，以来，計算機科学分野において最も広く引用される結果の一つとなったが，具体的な掛け算の OBDD サイズについては，その漸近的振る舞いすら明らかとなっていなかった．

本研究では，この問いに答えるべく，2 進 n 桁同士の掛け算を OBDD で表現するのに必要なサイズを理論と実験の両面から評価した．その結果，ベンチマークとして最も良く用いられる，n 桁同士の 2 進整数の掛け算の中心の桁 (n 桁目) はサイズが $O(2^{6n/5})$ の OBDD で計算できることを明らかにした．これは，従来知られるサイズの上界を改良するものである．また，小さな入力桁数に対して，掛け算を表現する最適な OBDD を実際に計算機実験により構成することで，上で示した上界の性能を評価した．その結果，n 桁の掛け算の中心桁を表現する最適な OBDD のサイズは $2^{6n/5}$ にほぼ比例すること，すなわち，本研究で得たサイズの上界がほぼ最適であることを強く示唆する結果を得た．また，同様に掛け算の各桁の表現サイズについても評価し，従来知られるものより優れた上界を得た．サイズの下界に対する理論的証明を与えることが，本問題に対する特に大きな課題として残されている．

しきい値回路とは，線形しきい値素子を用いて構成される非周期的回路である．しきい値回路は，単純化した脳のモデルとして，その計算能力について，古くより盛んな研究が行われている．線形しきい値素子は，入力の重み付き線形和が，ある値を超えるか否かにより 0 または 1 を出力する論理素子として定義されるが，ここで用いられる重みの許容範囲の大小が，素子あるいはこれを組み

合わせて得られる回路の計算能力に影響を与えることが知られている．本研究では，この現象をより厳密に解析するため，段数が少ないしきい値回路に着目し，その中で用いられる素子の重みの大小と，計算能力の関係について精査した．

その結果，出現する重みに制限を設けない任意の線形しきい値関数を計算する，二層の多項式的重みしきい値回路の効率的な構成手法を与えることに成功した．更に，2 進 n 桁の数同士の足し算，あるいは比較といった基本的な演算に対する，二層の多項式重みしきい値回路の構成に関して，従来知られるデルタ多項式と呼ばれる代数的式の性質を用いた構成法に比べ，剰余系の性質を利用した数論的手法がより効率的な回路を与えることを明らかにした．

現在，重みに制限を設けない多項式サイズの二層のしきい値回路の計算能力がクラス NP よりも真に弱いことを証明する問題が，計算の複雑さの理論における最重要課題の一つとなっている．対して，重みを多項式的に制限した回路に対する同様の問題は，古く 80 年代後半に解決を見た．したがって，しきい値回路における重みの大小と計算複雑さの関係の解明を試みる本研究のアプローチは，上記課題の解決に向けた有望なものと考えている．

研究業績一覧

学術論文

1. Eiji Takimoto, Syuhei Koya, Akira Maruoka:
   “Boosting Based on Divide and Merge”, Proceedings of the 15th International Conference on Algorithmic Learning Theory (ALT 2004), Lecture Notes in Artificial Intelligence, 3244, 127–141, Oct. 2004.
   概要: InfoBoost is a boosting algorithm that improves the performance of the master hypothesis whenever each weak hypothesis brings non-zero mutual information about the target. We give a somewhat surprising observation that InfoBoost can be viewed as an algorithm for growing a branching program that divides and merges the domain repeatedly. We generalize the merging process and propose a new class of boosting algorithms called BP.InfoBoost with various merging schema. BP.InfoBoost assigns to each node a weight as well as a weak hypothesis and the master hypothesis is a threshold function of the sum of the weights over the path induced by a given instance. InfoBoost is a BP.InfoBoost with an extreme scheme that merges all nodes in each round. The other extreme that merges no nodes yields an algorithm for growing a decision tree. We call this particular version DT.InfoBoost. We give an evidence that DT.InfoBoost improves the master hypothesis very efficiently, but it has a risk of overfitting because the size of the master hypothesis may grow exponentially. We propose a merging scheme between these extremes that improves the master hypothesis nearly as fast as the one without merge while keeping the branching program in a moderate size.

2. Nobuyoshi Sato, Minoru Udagawa, Minoru Uehara, Yoshifumi Sakai, Hideki Mori:
   “Redundant Architecture in Cooperative Search Engine”, Journal of Applied Systems Studies, vol. 5, no. 2, 157–168, Jul. 2004.
   概要: We have developed a distributed search engine, called Cooperative Search Engine (CSE), in order to retrieve fresh information. In CSE, a local search engine located in each Web server makes an index of local pages, and a meta search server integrates these local search engines in order to realize a global search engine. This meta server is a single point of failure in CSE. Therefore, we propose the introduction of redundancy for the meta search servers in order to increase the availability of CSE. In this paper, we describe and evaluate a reliable architecture for CSE.

3. Kazuyuki Amano, Akira Maruoka:
"On Learning Monotone Boolean Functions under the Uniform Distributions", Theoretical Computer Science, (掲載予定) .
概要: In this paper, we prove two general theorems on monotone Boolean functions which are useful for constructing a learning algorithm for monotone Boolean functions under the uniform distribution. A monotone Boolean function is called fair if it takes the value 1 on exactly half of its inputs. The first result proved in this paper is that a single variable function $f(x) = x_i$ has the minimum correlation with the majority function among all fair monotone functions. This proves the conjecture by Blum, Burch and Langford (1998, Proc. 39th FOCS, pp.408–415) and improves the performance guarantee of the best known learning algorithm for monotone Boolean functions under the uniform distribution they proposed. Our second result is on the relationship between the influences and the average sensitivity of a monotone Boolean function. The influence of variable x_i on f is defined as the probability that $f(x)$ differs from $f(x \oplus e_i)$ where x is chosen uniformly from $\{0,1\}^n$ and $x \oplus e_i$ means x with its i-th bit flipped. The average sensitivity of f is defined as the sum of the influences over all variables x_i. We prove that a somewhat unintuitive result which says if the influence of every variable on a monotone Boolean function is small, i.e., $O(1/n^c)$ for some constant $c > 0$, then the average sensitivity of the function must be large, i.e., $\Omega(\log n)$. We also discuss how to apply this result to the construction of a new learning algorithm for monotone Boolean functions.

4. Kazuyuki Amano, Akira Maruoka:
"On the Monotone Circuit Complexity of Quadratic Boolean Functions", Proceedings of the 15th International Symposium on Algorithms and Computation (ISAAC 04), Lecture Notes in Computer Science, 3341, 28–40, Dec. 2004.
概要: Several results on the monotone circuit complexity and the conjunctive complexity, i.e., the minimal number of AND gates in monotone circuits, of quadratic Boolean functions are proved. We focus on the comparison between single level circuits, which have only one level of AND gates, and arbitrary monotone circuits, and show that there is a huge gap between the conjunctive complexity of single level circuits and that of general monotone circuits for some explicit quadratic function. Almost tight upper bounds on the largest gap between the single level conjunctive complexity and the general conjunctive complexity over all quadratic functions are also proved. Moreover, we describe the way of lower bounding the single level circuit complexity, and give a set of quadratic functions whose monotone complexity is strictly smaller than its single level complexity.

研究会等

1. Shigeaki Harada, Eiji Takimoto, Akira Maruoka:
"Online Allocation with Risk Information", Proceedings of the 4th Japanese-Hangarian Symposium on Discrete Mathematics and Its Applications, (発表予定) .
概要: We consider the problem of dynamically apportioning resources among a set of options in a worst-case online framework. The model we investigate is a generalization of the well studied online learning model. In particular, we allow the learner to see as additional information how high the risk of each option is. This assumption is natural in many applications like horse-race betting, where gamblers know odds for all options before placing bets. We apply the Aggregating Algorithm to this problem and

give a tight performance bound. The bound we give intuitively implies that the algorithm performs better when faced with options of various risks than when faced with options of the same risk.

2. 瀧本 英二:
"オンライン予測の理論と応用", 第 18 回 回路とシステム軽井沢ワークショップ予稿集, (発表予定).
概要: オンライン予測と呼ばれる普遍的な意思決定モデルの方法論について概説する. このモデルは適用範囲が極めて広く, 符号理論, ゲーム理論, 学習理論, ファイナンス理論, オンライン最適化理論などさまざまな分野の問題を統一的に扱う枠組みを提供する. さらに, 各分野で得られた結果の多くは, 1 つの戦略スキームを用いて説明することができる. 本講演では, 戦略スキームの原理について述べた後, それが各分野でどのように応用されているかを紹介する.

3. Nobuyoshi Sato, Minoru Uehara, Yoshifumi Sakai:
"A Case Study on Freshness based Scoring for Fresh Information Retrieval", Proceedings of IEEE International Symposium on Communications and Information Technologies 2004, 210–215, Oct. 2004.
概要: For most businesses, fresh information retrieval is very important. However, it is difficult for conventional search engines based on centralized architecture to retrieve really fresh information, because they take a long time to collect documents via Web robots. In contrast to a centralized architecture, a search engine based on a distributed architecture does not need to collect documents, because each site independently makes an index. As this result, distributed search engines can retrieve really fresh information. However, fast indexing is not enough to easily retrieve fresh information. The value of information is determined by both freshness and relevance. Traditional ranking methods consider either freshness or relevance; so, we proposed FTF·IDF (Fresh Term Frequency multiplied by Inverse Document Frequency) as a scoring method that considers both freshness and relevance. In this paper, we will describe a verification of FTF·IDF on an actual web diary.

4. Kazuyuki Amano, Akira Maruoka:
"Tighter Bounds on the OBDD Size of Integer Multiplication", Proceedings of the 4th Japanese-Hangarian Symposium on Discrete Mathematics and Its Applications, (発表予定) .
概要: We show that the middle bit of the multiplication of two n-bit integers can be computed by an OBDD of size less than $2.8 \cdot 2^{6n/5}$. This improves the previously known upper bound of $(7/3) \cdot 2^{4n/3}$ by Woelfel (STACS, 2001). The experimental results suggest that our exponent of $6n/5$ is (at least very close to) optimal. A general upper bound of $O(2^{3n/2})$ on the OBDD size of each output bit of the multiplication and some conjecture on the structural properties of multipliers inspired by the experimental results are also presented.

5. Kazuyuki Amano, Akira Maruoka:
"Better Simulation of Exponential Threshold Weights by Polynomial Weights", Electronic Colloquium on Computational Complexity, 10, 90-1–90-8, Nov. 2004.
概要: We give an explicit construction of depth two threshold circuit with polynomial weights and $\tilde{O}(n^5)$ gates that computes an arbitrary threshold function. We also give the construction of such circuits with $O(n^3/\log n)$ gates computing the COMPARISON and CARRY functions, and that with $O(n^4/\log n)$ gates computing the ADDITION function. These improve the previously known constructions on its size and simplicity.

学会大会等

1. 天野 一幸:
   “しきい値素子を用いた回路における計算量について”, 日本オペレーションズ・リサーチ学会関西支部研究部会, 2005 年 1 月.

A02: 計算理論的設計による知識抽出モデルに関する研究

徳山　豪　　塩浦昭義

東北大学 大学院 情報科学研究科
〒 980-8579 仙台市青葉区荒巻字青葉０９
{tokuyama,shioura}@dais.is.tohoku.ac.jp

1　はじめに

本研究の目的はデータマイニングにおける現在の精度限界を打破するための知識抽出モデルの提案と、それに関する理論研究及び実際のシステムの構築である。　特に、研究代表者の持つ先端技術である計算幾何学的手法を中心に、計算理論手法による限界突破を目指す。データマイニングは大規模なデータから情報をコンパクトな知識として抽出する技術であり，近年に情報科学から発信した技術であるにもかかわらず、経済学，経営学、統計学などの学問分野、及び経営コンサルティング、在庫管理や顧客サービスといった実用分野に幅広く応用が期待され、情報化社会における最重点技術の一つである。

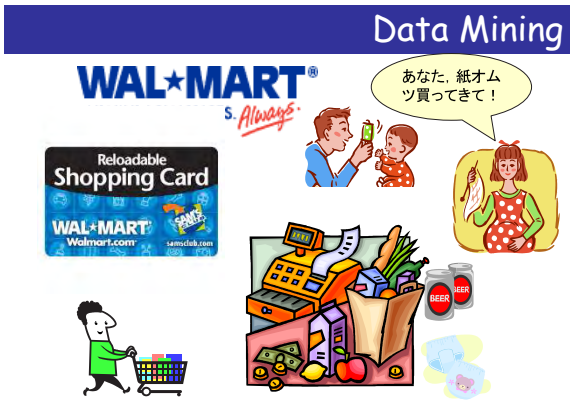


図 2.1: データマイニングのイメージ：紙おむつを買う人は高い確率でビールも同時に買う

自動的に抽出し、表示された知識形態は、ユーザにより意志決定等の補助として用いられる。重要な条件は、抽出した知識形態がシンプルであり（単純性）、正確にデータの特性を記述すること（正確性）、知識として（サンプルに依存しない）汎用性を持つ事（学習汎用性）さらにユーザにとって説得力があり、検証が容易であること（透明性）である。単純性と透明性の観点から、結合ルール及びそれを用いた決定木は有力な手法である。これらの手法を用いたデータマイニングの研究は IBM 社アルマデン研究所や米国スタンフォード大学、カナダ国サイモンフレーザー大学、オーストラリア国シドニー大学等で 1980 年代半ばに始まり、主に二値データに対する研究が行われた。スタンフォード大学での研究成果の一例として、スーパーマーケットの売上情報のデータのマイニングでの「紙おむつを買う人はビールを買う」といったルールは広く知られている。これは、どちらかというとネガティブなイメージ（くだらないルールしか発見できない）に捉えられがちだが、「常識からは見出せないルールも発見できる」と見るべきである。現在では、広くデータマイニング技術は用いられており、例えば本のインターネット販売でも、データマイニングを用いた解析により、購買者の過去の履歴から、興味のありそうな書籍のリストを作成して提示するというような事が行われている。

さて一方、実用データマイニングで必須である数値データベースの取り扱いを考えると、数値データの二値化誤差から生じる、正確性と学習汎用性のトレードオフに関する精度限界があり、それを乗り越えるのは技術的に困難と思われていた。日本でのデータマイニングの研究はこれに数年遅れ、研究代表者を含む日本 IBM のチームが 1990 年代後半に行った研究が国際的に最初に認められた成果である。具体的には、結合ルール条件生成時のアダプティブな二値化のアイデアを導入し、二値化誤差最小化の理論的枠組みである最適結合ルールの定式化を与え、データマイニングに計算理論の手法を導入することに世界に先駆けて成功

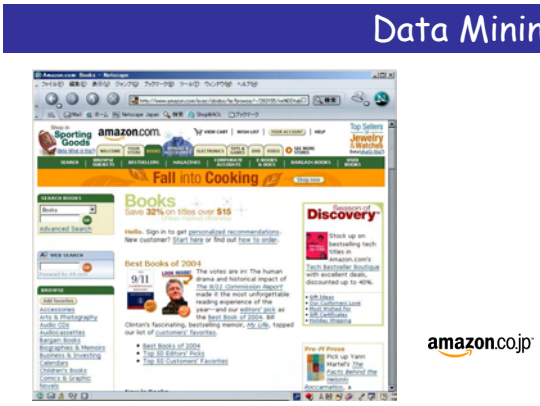


図 2.2: 書籍販売でのデータマイニング

した（1996-1998 年）．これにより、上記のトレードオフは大きく改善された。世界的に独創的な研究として高く評価され、現在広く関連研究がなされている。　しかしながら、最小誤差二値化を用いても誤差には理論的下界があり、上記限界の完全な克服には至っていない。本研究では、透明性を保ちながら、この二値化誤差からくる限界を克服するデータマイニングシステムの設計とその理論的解析を行う。　このようなデータマイニングシステムは要望されてはいるが、現実化は難しく、独創的な新しいアイデアが必要とされていた。

本研究により、既存の多くのデータマイニングシステムの重要なコンポーネントである意志決定システムに透明性と高い学習汎用性が与えられると予想される。更に、基本技術として用いるグラフ・計算幾何アルゴリズム理論を中心とした理論計算機科学での理論発展と共に、理論計算機科学技術の知識抽出への応用の新しい進展が期待される。

2　初年度の計画と成果

上述のように本研究では、透明性を保ちながら、二値化誤差からくる限界を克服するデータマイニングシステムの設計とその理論的解析を行う。
初年度、次年度の具体的な成果目標としては　階層化ルールをエキスパートとして用いた柔軟な決定木の実現がメインであり、初年度は、そのコンポーネント技術の開発とプロトタイプ作成をターゲットとした。

初年度の具体的な成果としては、下記のものがある。論文等の番号は研究業績一覧に対応する。

1. 柔軟な決定木の構築に用いる階層ルールの高次元におけるモデル化と高速アルゴリズムの設計及び最適データ近似の研究。（学術論文 6,7,8,9, 研究会発表３）

2. データマイニングでの主要な道具であるクラスタリングにおいて、クラスタ発見の高濃度部分グラフ問題としての定式化と、計算クラスに関する新しい発見。（研究会発表１、学会大会　５）

3. 階層化ルールをエキスパートとして用いた柔軟な決定木のプロトタイプ実装を行い、実験による評価の開始。（研究会発表 4,7、学会大会３，４）

4. インターネットにおける知識抽出の実用的なモデル化の側面から、クラスタリングのモデルに対する検討及び実用的定式化の研究と実装。（研究会発表 5,8,9）

5. データサンプリングに関する離散システム理論とアルゴリズム理論の研究成果。（学術論文 1、2、3、4、研究会発表２）

その他、経済予測でのモデル化とアルゴリズム理論の応用、また、最適化の基礎理論である離散凸解析の理論などにおいても成果をあげた。

3　研究活動

研究活動予定に従い、徳山は基礎理論とモデル化及び計算限界の算定、塩浦は数理最適化とアルゴリズム理論に絞って研究を開始した。システム実装と実験に関しては、大学院博士課程の学生全眞嬉（平成 17 年度は学術振興会特別研究員に採用）を中心に大学院学生のプロジェクトを構成し実施した。

研究代表者の徳山は研究成果に関連した論文誌・査読付き国際学会論文を 10 本、研究協力者の塩浦は同 7 本（徳山との共著を除く）発表している。その他、国内学会、研究会等での発表も数多く行った。　徳山は本特定研究主催の NHC 国際会議の

PC 委員長として活動し、多くの国際的な研究者を招聘すると共に、活発な国際交流を行った。塩浦は同国際会議で成果発表も行っている。

理論的な研究が主体であるため、研究活動に必須である国際的活動と、仙台からの国内旅費の必要性から、小規模な備品・消耗品を除き研究費のほとんどは旅費に宛てた。特に NHC 国際会議には、プロジェクトに参加する学生を参加させ、国際的な一流研究者との交流経験を積ませたが、その旅費も本研究費から拠出した。また、徳山は SWAT 国際会議、ISAAC 国際会議、COCOON 国際会議などのアルゴリズム分野でのシリーズ国際会議で研究成果を発表し、また、共同研究を行い、広く国際的に活動した。塩浦は SODA 国際会議等で広く情報収集・共同研究を行ったほか、国内研究者のセミナー等で最先端の研究活動に中心的な役割を果たした。また、特定研究の研究費で J. Matousek、M. Halldorsson ら国際的に一流の研究者に東北大学において講演・共同研究を依頼し、成果をあげている。

特筆すべきこととして、徳山は平成 17 年 3 月には本特定領域に直接関連するテーマ「計算幾何学の理論研究と、データマイニングにおける先駆的研究への応用」で船井情報科学財団から船井情報科学振興賞を受賞し、研究レベルが高く評価されている事を示した。

4 研究成果の概要

4.1 階層ルールの高次元におけるモデル化とアルゴリズム設計

データベースからの知識抽出システムの構成において、数値属性の取り扱いは大きなトピックである。数値属性の 2 値化に関しては、さまざまな研究があり、特に数値属性のペアについては領域ルールというアイデアが福田-森本-森下-徳山によって 1996 年（SIGMOD96）に考案され、大きな効果を上げている。しかし高次元（多属性）領域ルールの実現にあたっては、直接的なモデル化を行うと、近似計算すら困難な問題に定式化される。

この計算困難性を避けるために計算理論的な考察を行い、それに従ったモデル化とアルゴリズム設計を行う必要性がある。更に進んで 2 値化ではなく柔軟な多値化によって得られる階層化ルールは後述のように、エキスパート付きの決定木構築に重要な役割を果たすが、1 次元の場合にのみ良い手法が考案され、　1 次元手法の直接的な拡張は多項式時間アルゴリズムにならないという問題点があった。実際、高次元（多属性）階層化ルールの実現にあたっては、直接的なモデル化を行うと、近似計算すら困難な問題に定式化される。

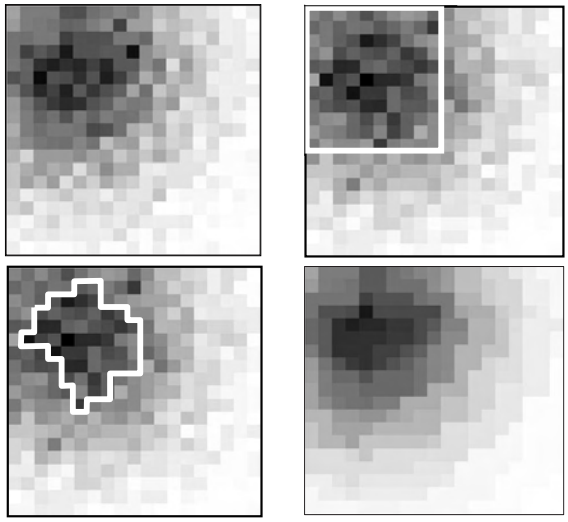


図 2.3: 2 種類（長方形、ピクセル凸）の領域ルールと階層化ルール（右下図）

この計算困難性を避けるために計算理論的な考察を行い、それに従ったモデル化とアルゴリズム設計を行う必要性がある。　この困難を克服するために、本研究ではボクセルグリッド上で定義された単峰曲面によるデータ分布の近似として問題を定式化した。さらに有向グラフを用いて任意の次元における高次元ルールをモデル化し、階層化された領域ルールの最適化問題を最大支配カットというネットワークフロー問題に帰着し、高速アルゴリズムの設計を実現した。これは、一般次元での数値属性のアソシエーションルールの設計としては世界初であり、大きな成果である。　図 2.3 では、2 次元の例で、ピクセルグリッドの濃度がデータの確信度分布、左上と右下が領域ルール。右下図が階層化された領域ルールであり、濃度を高さと思うと曲面の等高線表示を示している。
正確にはデータマイニングで利用する際は、ピクセルグリッドにはサポートに対応した非均一な測

度を導入し、この測度に対して最適化を行う。そのため、我々の手法は任意の測度に対して有効であるように設計されている。図 2.4 では対応するグラフと最大支配カットを示す。さらに二次元の

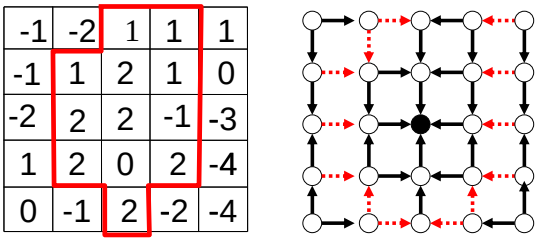


図 2.4: 領域の切り出し（左図）と対応するグラフの最大支配カット（右図）

階層化ルールにおける計算量の改善、一般の L_p 基準による 1 次元の階層化ルールの最適アルゴリズム設計なども成果としてあげられる。更に、1 次元データに関しては、データの確信度分布のヒストグラムから最適の k ピーク近似を計算するアルゴリズムを開発し、これにより、データから幾つのルールを抽出すべきかの判定、隠れた比較的小さいルールの抽出が可能となった。

また、1 次元ルールの設計に関連して、ピークの数ではなく区分線形関数の折れ線の数に注目し、尺度を L_1 もしくは L_2 にした、データ集合の最適折れ線近似に対しても新しい理論成果をあげた。これは、従来 L_∞ 基準でしか考えられていなかった折れ線近似問題に新しい定式化を与えたものである．これらの成果は COCOON, ISAAC 等の国際会議で発表し、論文誌にも投稿中である。

4.2 高濃度部分グラフを用いたクラスタリング

知識抽出システムでは重複を許した非排他的クラスタリングが重要な Tool である。そこでは、データを分割するのではなく、クラスタを一つづつ発見していくというアプローチが採られる。代表的なアルゴリズムとしてしられる Agrawal らのアプリオリアルゴリズムは、データと（カテゴリ）属性の作る二部グラフを考え、データ部分の大きい 2 部クリーク（完全二部グラフ）を全て列挙するという方針をとっている． しかしながら、この手法では属性数の多いクリークを求める事は計算爆発により不可能である。改良として極大 2 部クリーク列挙アルゴリズムも提案されているが、計算爆発を完全には克服できない。一方、枝数が最大のクリークを求める問題、もしくは指定した属性数に対する最大クリークを求める問題は NP 完全であり、近似する事も計算量理論的に困難である。従って、本研究では、クリークではなく、（サイズを指定した）最大濃度部分グラフ問題を用いてクラスタ発見を行うという新しいアプローチを採る。最大濃度部分グラフ問題は古くから研究されている。従来の計算理論の研究においては、U.Feige によってランダム３ＳＡＴ判定からの帰着が示されており、計算量は近似困難問題のクラスに入り多項式時間アルゴリズム設計は（計算階層が崩壊しない限り）不可能であった。知られている最良の近似比は $O(n^{1/3})$ を少し改良したもの（Feige ― Kortsarz-Peleg, Algorithmica 1993）であり、これを越えることは非常に難しいとされていた。 多項式時間の定数近似アルゴリズム設計が可能な既知の場合は、Arora-Karger-Karpinski らによる部分グラフが $\Omega(n^2)$ の辺数を持つ場合（STOC95）の PTAS があるが、これは実用的に利用できない。また、朝廣-岩間-玉木-徳山によるグリーディーアルゴリズムの解析（J. Algorithms 2000）では、定数近似を達成するのは頂点数が $\Omega(n)$ の場合に限られていた。一方、本研究では、最大濃度部分グラフの濃度に注目し、この濃度が高い（クリークに比べて定数倍の辺を持つ）場合は、高速な近似アルゴリズムの設計が可能であることを示した。この高濃度条件は、データマイニングのようにクリークに近い部分グラフのみを必要とする場合には実用的に妥当な条件である。

成果としては、二部グラフに対しては $O(n^\epsilon)$ 近似アルゴリズムおよび擬多項式時間近似スキームを与え、この近似スキームが多項式時間近似スキームになるための条件の明確な提示を行った。これらは、新しい見地から最大濃度部分グラフ問題の計算量を追求したものであり、世界的にも新規性の高い成果である。

更に二部グラフでない一般のグラフや重み付きグラフに対してもこの理論を拡張し、$O(n^{\epsilon})$ 近似の多項式時間アルゴリズム及び 2 近似を達成する擬多項式時間アルゴリズムを考案している、成果は研究会で発表の外、来年度国際的な会議で発表する予定である。

4.3 エキスパート付き決定木の構成と実装

アソシエーションルールを用いた決定木はデータマイニングにおける意思決定システムとして広く用いられている。しかしながら、数値属性を含むデータにおいては、データのカテゴリ属性への変換による情報損失があり、この損失と決定木における過学習のバランスを取る事が重要になる。そのために、数値属性の情報をエキスパートとして付加した決定木を構成する。エキスパート付き決定木に関しては主に学習理論の見地から理論的な研究は行われているが、現実のエキスパートの作成を階層化ルールを用いて実現し、数値データベースでのデータマイニングへの応用を意識した実装実験を行ったのは世界でも初めてのものである。

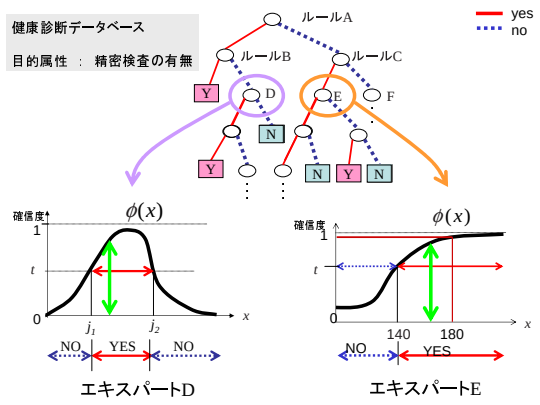


図 2.5: エキスパート付き決定木

最適ピラミッドを用いた決定木構成アルゴリズムは以下のようになっている．

step1 学習データ T を読み込む．

step2 T のすべての事例が同一クラスならば葉とする．
そうでなければ，各属性に対して次の 1〜4 を行う．

1. 各属性値における確信度を求める．
2. 求めた確信度を元に最適ピラミッドを構築する．
3. 全ての高さに対して分割を行い，相互情報量を計算する．
4. 得られた各属性の相互情報量を比較する．
   (a) 閾値 g_ℓ 以上かつ最も大きな相互情報量が得られた属性があるならば，それをノードとし，T を T_1，T_2 に分割する．同時に，T_1，T_2 の確信度を求めておく．
   (b) もし，どの属性の相互情報量も g_ℓ 未満であるならば，T に最も多く現れるクラスラベルの葉とする．
5. 分割頂点に最適ピラミッドから構成したエキスパートを配備する

step3 分割された事例集合に対し，全てが葉になるまで **step1**，**step2** を繰り返す．

生成された決定木の各ノードでは分割テストが行われる．例えば，根である属性 A テストは，全学習データ T の，属性 A について求められた確信度のヒストグラム f を持つ．また，f から求められた最適ピラミッド ϕ，そして，分割された T_1，T_2 の確信度 $conf(T_1)$，$conf(T_2)$ をそれぞれ持っている．この確信度はテストデータが分類され，枝を通るときに各テスト事例に対して与えられる．分割された事例集合 T_1，T_2 は，子ノードに入力され，子ノードも同様な構造を持つ．

また，決定木の末端である葉には，クラスラベルが与えられる．その葉に振り分けられた学習データの事例数 $|T_{11}|$，その中でクラスが C でない事例数 $|E_{11}|$ (エラー数) も記録してある．

エキスパートは，決定木構築アルゴリズムの **step2**.4 の後に生成され，該当ノードにおける学習データ数 $|T|$，及び，T より構築された最適ピラミッド関数 $\phi(T)$ を持つ．エキスパートは決定木の各ノードに配置される．入力されたデータ i に対し，ノード A のエキスパートは，学習データ数 $|T|$，及び $\phi(T)$ におけるデータ i の確信度 $\alpha_T(i)$，を与える．そして，与えられた確信度と事例数の

セットにより，データ i のクラスを決定できるかどうか判断する．あるノード A の情報の信頼性が大きいと判断し，そこでデータ i にラベルを与え，テストを終了する判断を行う．即ち，ノード A, B 間で枝刈りを行うことになる．ここで，比較に用いた $\alpha_T(i)$ の値は各データによって値が異なる．つまり，エキスパートは，個々のデータに依存した，データごとに柔軟かつインプリシットに決定木の枝刈りを行う．

実験では、C4.5 が生成した枝刈り前の決定木の各ノードに最適ピラミッドを構築し，エキスパートを配置した．各ノードのエキスパートは，テストデータに対し，個々のデータに依存する確信度を与える．その確信度がユーザの指定した範囲にあれば，その時点でラベルを与え，分類を終了し，次のデータの分類へと進む．実験データはUCIで提供するDiabetesデータセット (http://www.ics.uci.edu/ mlearn/MLRepository.html) で，糖尿病診断データをもちいた．初年度での実装実験は予備的なものであり、研究会等での発表にとどまっているが、実験ではエキスパートのパラメタと精度の相関を調べ、パラメタをチューンする事によりエキスパートなしの場合に比べて精度の大幅な向上を見ることが出来た。

4.4 インターネットでの探索における知識抽出

インターネットでの検索エンジンは現代生活に不可欠なものとなっている。現在、検索エンジンにより得られた検索結果はページランクアルゴリズムなどにより整列され、リストとして表示される。 しかしながら， WWW の巨大化と検索の高速化・大規模化に伴い、検索結果として得られた文書集合を知識抽出により判りやすい形で分類し、表示する技術が必要になってきている。さまざまなクラスタリング手法による分類が考えられているが、本研究では、Latent Semantics を用いた文書集合の非排他的クラスタリングを行う時に、クラスタに自動的に付随するラベルを知識として捉える。 これにより、ラベルに関して排他的であり文書に関して非排他的であるクラスタリングをネットワークフローなどを用いて考察し、

従来よりも利用しやすい検索エンジン（LBHC: Label Based Hierachical Clustering 法) の設計を行った。プロトタイプの実験結果は研究会等で発表している。

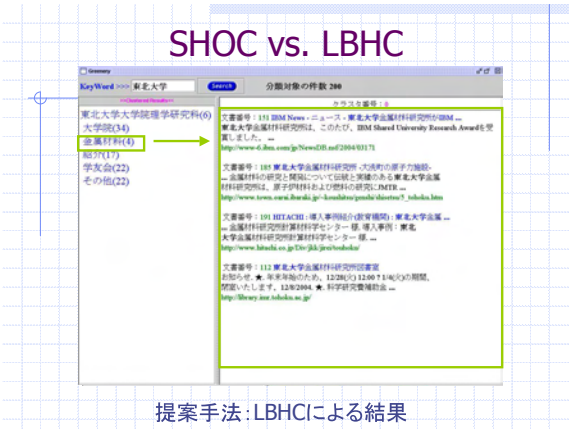


図 2.6: 排他的ラベルクラスタによる検索結果表示

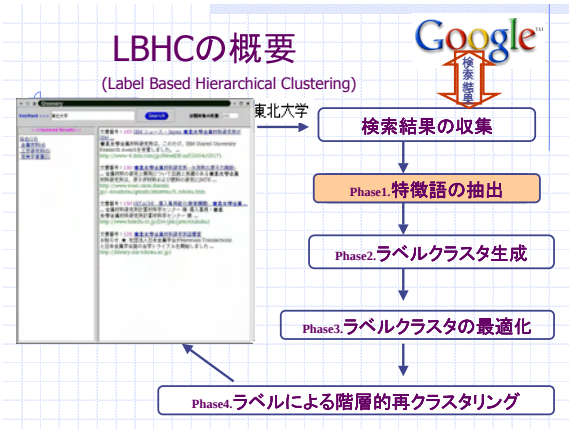


図 2.7: システム構成

4.5 データサンプリングと最適近似に関する理論研究

データ圧縮及びデータサンプリングで重要である丸めとディスクレパンシー基準による最適性評価において、計算理論的な成果をあげた。特に、グラフの最短路と幾何学的領域族に関するハイパーグラフに対する大域丸め集合の離散的構造を解明し、その列挙アルゴリズムの設計を行った。 特に領域族に対する丸め理論は、幾何学データの圧縮とサンプリングに応用があると期待される。こ

れらの成果は本研究のテーマに間接的に影響を及ぼすものであり、海外の一流論文誌、一流国際会議で発表している。

研究業績一覧

学術論文

1. J.Jansson, T. Tokuyama :
"Semi-Balanced Coloring of Graphs: Generalized 2-Coloring Based on a Relaxed Discrepancy Condition", Graphs and Combinatorics, 20, 205-222, 2004.
概要: Let G be an undirected, unweighted, connected graph with n vertices and m edges. We introduce the concept of a semi-balanced coloring of G, which is a 2-coloring of the shortest-paths hypergraph of G under a certain discrepancy condition yielding a class of independent sets of G. We prove that the number of different semi-balanced colorings of G is: (1) at most $n+1$ if G is bipartite; (2) at most m if G is non-bipartite and triangle-free; and (3) at most $m+1$ if G is non-bipartite. Based on the above combinatorial investigation, we design an algorithm that enumerates all semi-balanced colorings in $O(nm^2)$ time.

2. T. Asano, N. Katoh, H. Tamaki, T. Tokuyama :
"The Structure and Number of Global Roundings of a Graph", Theoretical Computer Science, 325, 425-437, 2004.
概要: Given a connected weighted graph $G = (V, E)$, we consider a hypergraph $H_G = (V, P_G)$ corresponding to the set of all shortest paths in G. For a given real assignment $\mathbf{a}$ on V satisfying $0 \leq \mathbf{a}(v) \leq 1$, a global rounding α with respect to H_G is a binary assignment satisfying that $|\sum_{v \in F} \mathbf{a}(v) - \alpha(v)| < 1$ for every $F \in P_G$. We conjecture that there are at most $|V|+1$ global roundings for H_G, and also the set of global roundings is an affine independent set. We give several positive evidences for the conjecture.

3. K. Sadakane, N. Takki-Chebihi, T. Tokuyama :
"Combinatorics and Algorithms for Low-Discrepancy Roundings of a Real Sequence", Theoretical Computer Science, 331, 23-36, 2005.
概要: We discuss the problem of computing all the integer sequences obtained by rounding an input sequence of n real numbers such that the discrepancy between the input sequence and each output binary sequence is less than one. The problem arises in the design of digital halftoning methods in computer graphics. We show that the number of such roundings is at most $n + 1$ if we consider the discrepancy with respect to the set of all subintervals, and give an efficient algorithm to report all of them. Then, we give an optimal method to construct a compact graph to represent the set of global roundings satisfying a weaker discrepancy condition.

4. T. Ishikawa, K. Kawarabayashi, T. Tokuyama :
"On Properties of a Set of Global Roundings Associated with Clique Connection of Graphs", Interdisciplinary Information Sciences , 10-2, 159-163, 2004.
概要: Given a connected weighted graph $G = (V, E)$, we consider a hypergraph $H(G) = (V, F(G))$ corresponding to the set of all shortest paths in G. For a given real assignment $\mathbf{a}$ on V satisfying $0 \leq \mathbf{a}(v) \leq 1$, a global rounding α with respect to $H(G)$ is a binary assignment satisfying that $|\sum_{v \in F} \mathbf{a}(v) - \alpha(v)| < 1$ for every $F \in F(G)$. Asano *et al.* conjectured that there are at most $|V| + 1$ global roundings for $H(G)$. In this paper, we present monotone properties on size and affine corank of a set of global roundings

under a clique connection operation.

5. T. Tokuyama :
"Minmax Parametric Optimization Problems and Multidimensional Parametric Searching", Interdisciplinary Information Scinences, 11-1, 1-9, 2005.
概要: The parametric minimax problem, which finds the parameter value minimizing the weight of a solution of a combinatorial maximization problem, is a fundamental problem in sensitivity analysis. Moreover, several problems in computational geometry can be formulated as parametric minimax problems. The *parametric search* paradigm gives an efficient sequential algorithm for a convex parametric minimax problem with one parameter if the original non-parametric problem has an efficient parallel algorithm. We consider the parametric minimax problem with d parameters for a constant d, and solve it by using multidimensional version of the parametric search paradigm. As a new feature, we give a feasible region in the parameter space in which the parameter vector must be located. Typical results obtained as applications are: (1) Efficient solutions for some geometric problems, including theoretically efficient solutions for the minimum diameter bridging problem in d-dimensional space between convex polytopes. (2) Solutions for parametric polymatroid optimization problems, including an $O(n \log n)$ time algorithm to compute the parameter vector minimizing k-largest linear parametric elements with d dimensions.

6. D. Chen, J. Chun, N. Katoh, T. Tokuyama :
"Efficient Algorithms for Approximating a Multi-Dimensional Voxel Terrain by a Unimodal Terrain", Proceedings of 10th Computing and Combinatorics Conference, Springer LNCS, LNCS3126, 238-248, 2004.
概要: We consider the problem of approximating a function on a d-dimensional voxel grid by a unimodal function to minimize the L_2 approximation error with respect to a given measure distribution on the grid. The output unimodal function gives a layered structure on the voxel grid, and we give efficient algorithms for computing the optimal approximation under a reasonable assumption on the shape of each horizontal layer. Our main technique is a dominating cut algorithm for a graph.

7. B. Aronov, T. Asano, N. Katoh, K. Mehlorn, T. Tokuyama :
"Polyline Fitting of Planar Point Set Under Min-Sum Criteria", Proceedings of 15th International Symposium on Algorithms and Computation, LNCS3341, 77-88, 2004.
概要: Fitting a curve of a certain type to a given set of points in the plane is a basic problem in statistics and has numerous applications. We consider fitting a polyline with k joints under the min-sum criteria with respect to L_1- and L_2-metrics, which are more appropriate measures than uniform and Hausdorff metrics in statistical context. We present efficient algorithms for the 1-joint versions of the problem, and fully polynomial-time approximation schemes for the general k-joint versions.

8. T. Asano, N. Katoh, H. Tamaki, T. Tokuyama :
"On Geometric Structure of Global Roundings of Graphs and Range Spaces", Proceedings of 9th Scandinavian Workshop on Algorithms, Springer LNCS, LNCS3111, 455-467, 2004.
概要: Given a hypergraph $H = (V, F)$ and a $[0,1]$-valued vector $\mathbf{a} \in [0,1]^V$, its global rounding is a binary (i.e.,$\{0,1\}$-valued) vector $\alpha \in \{0,1\}^V$ such that $|\sum_{v \in f}(\mathbf{a}(v) - \alpha(v))| < 1$ holds for each hyperedge $f \in F$. We study geometric (or

combinatorial) structure of the set of global roundings of $\mathbf{a}$ using the notion of compatible set with respect to the discrepancy distance. We conjecture that the set of global roundings forms a simplex if the hypergraph satisfies "shortest-path" axioms, and prove it for some special cases including some geometric range spaces and the shortest path hypergraph of a series-parallel graph.

9. J. Chun, K. Sadakane, T. Tokuyama :
"Peak Reducing Fitting of a Curve under the L1 Metric", Proceedings of Japan Conference of Discrete Computational Geometry, 掲載予定.
概要: Given a function $y = f(x)$ in one variable, we consider the problem of computing a k-peaked curve $y = \phi(x)$ minimizing the L_1 distance between them. In other words, $\phi(x)$ has at most k local peaks and minimizes the area bounded by the curves $f(x)$ and $\phi(x)$. This gives extension of the authors' previous work on the unimodal (i.e., single-peaked) approximation for the L_2 distance.

10. K. Ohta, K. Sadakane, A. Shioura, T. Tokuyama:
"A Fast, Accurate and Simple Method for Pricing European-Asian and Saving-Asian Options", Algorithmica, （掲載予定）.
概要: We present efficient and accurate approximation algorithms for computing the premium price of Asian options. First, we modify an algorithm developed by Aingworth et al. in SODA 2000 for pricing the European-Asian option and improve its accuracy (both theoretically and practically) by transforming it into a randomized algorithm. Then, we present a new option named Saving-Asian option, whose merit is in the middle of European-Asian and American-Asian options, and show that our method works for its pricing.

11. K. Murota, A. Shioura:
"Fundamental Properties of M-convex and L-convex Functions in Continuous Variables", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E87-A, 1042-1052, 2004.
概要: The concepts of M-convexity and L-convexity, introduced by Murota (1996, 1998) for functions over the integer lattice, extract combinatorial structures in well-solved nonlinear combinatorial optimization problems. These concepts are extended to polyhedral convex functions and quadratic functions over the real space by Murota–Shioura (2000, 2004). In this paper, we consider a further extension to general convex functions. The main aim of this paper is to provide rigorous proofs for fundamental properties of general M-convex and L-convex functions.

12. S. Moriguchi, A. Shioura:
"On Hochbaum's Scaling Algorithm for the General Resource Allocation Problem", Mathematics of Operations Research, 29, 394–397, 2004.
概要: It is pointed out that the polynomial-time scaling algorithm by Hochbaum (1994) does not work correctly for the general resource allocation problem. We fix the algorithm so that it works correctly, and analyze the time complexity of the fixed algorithm.

13. A. Shioura:
"The MA-Ordering Max-Flow Algorithm is Not Strongly Polynomial for Directed Networks", Operations Research Letters, 32, 31–35, 2004.
概要: Quite recently, Fujishige (2003) developed a weakly polynomial-time algorithm for the maximum flow problem by applying the maximum adjacency (MA) ordering technique to directed networks. In this

note, we show that the algorithm is not strongly polynomial by giving a real-valued instance for which the algorithm does not terminate.

14. K. Murota, A. Shioura:
"Quadratic M-convex and L-convex Functions", Advances in Applied Mathematics, 33, 318–341, 2004.
概要: The concepts of L-convexity and M-convex are introduced by Murota (1996, 1998) for functions defined over the integer lattice, and then extended to polyhedral convex functions by Murota–Shioura (2000). In this paper, we consider these concepts for quadratic functions and investigate the structure of the coefficient matrices of such quadratic functions. It is shown that quadratic L-convex and M-convex functions can be characterized by nice combinatorial properties of their coefficient matrices.

15. K. Murota, A. Shioura:
"Conjugacy Relationship Between M-convex and L-convex Functions in Continuous Variables", Mathematical Programming, 101, 415–433, 2004.
概要: By extracting combinatorial structures in well-solved nonlinear combinatorial optimization problems, Murota (1996, 1998) introduced the concepts of M-convexity and L-convexity to functions defined over the integer lattice. Recently, Murota–Shioura (2000, 2004) extended these concepts to polyhedral convex functions and quadratic functions in continuous variables. In this paper, we consider a further extension to more general convex functions defined over the real space, and provide a proof for the conjugacy relationship between general M-convex and L-convex functions.

16. R. Farooq, A. Shioura:
"A Note on the Equivalence Between Substitutability and $M^\natural$-convexity", Pacific Journal of Optimization, 1, 243–252, 2005.
概要: The property of "substitutability" plays a key role in guaranteeing the existence of a stable solution in the stable marriage problem and its generalizations. On the other hand, the concept of $M^\natural$-convexity, introduced by Murota–Shioura (1999) for functions defined over the integer lattice, enjoys a number of nice properties that are expected of "discrete convexity" and provides with a natural model of utility functions. In this note, we show that $M^\natural$-convexity is characterized by two variants of substitutability.

研究会等

1. 鈴木晶子, 徳山豪:
"二部グラフの高濃度部分グラフ問題の近似アルゴリズムについて", 情報処理学会アルゴリズム研究会, 97, 17-24, 2004.
概要: 二部グラフの高濃度部分グラフ問題はさまざまな応用を持つが、従来近似困難とされていた。本論文では、出力グラフの濃度が高いという条件の元で、効率の良い近似アルゴリズムの設計を行った. このアルゴリズムはランダマイズドアルゴリズムであり、解析により一般に Pseudo-PTAS であり、広い場合に PTAS になることを示した。

2. 廣川裕, 徳山豪:
"チェッカーボード丸めに関する考察と実装", 電子情報通信学会コンピュテーション研究会, ２００５－１, 91-96, 2005.
概要: ２ｘ２小行列全体を領域空間としてみた時の行列丸めのディスクレパンシーのアルゴリズムの紹介と、新しい下界の提示

3. 結城匡人, 全眞嬉, 徳山豪:
"曲線のピーク削減アルゴリズムの考察と実装", 電子情報通信学会コンピュテーション研究会, ２００５－１, 83-90, 2005.
概要: 曲線のピーク削減に関する効率の良いアルゴリズムの提案と実装実験による検証

4. 全眞嬉, 金子法正,　定兼邦彦, 徳山豪:
“数値属性を用いたエキスパート付き決定木の構築”, 第四回データマイニングワークショップ, 29, 21-24, （2004）.
概要: 数値属性に対する単峰近似を用いてエキスパートを作成し、データマイニングにおける C4.5 決定木をベースとしたエキスパート付き決定木を構築した。実験により性能の向上を示した。

5. 丸山謙志、王冠超、徳山豪:
“Web 検索結果におけるクラスタリングアルゴリズムの研究　”, 情報処理学会アルゴリズム研究会, 100, （発表予定）.
概要: WEB 検索におけるクラスタリングで、ラベルクラスタの精密化をネットワークフローを用いて行い、従来より利用しやすいクラスタリングシステムを試作した。さらにラベルによる排他的クラスタリングと文書の非排他的クラスタリングを組み合せて実用的なシステム設計を行った。

6. 塩浦 昭義, 徳山 豪:
“Efficiently Pricing European-Asian Options: Ultimate Implementation and Analysis of the AMO Algorithm”, 情報処理学会アルゴリズム研究会, 96, 43–50, 2004 年 7 月.
概要:　We propose an efficient and accurate randomized approximation algorithm for computing the price of a European-Asian option on the binomial tree model. For an option with the strike price X on an n-step binomial tree and any positive integer k, we give an $O(kn^2)$ time algorithm with the error bound $O(X/k)$ which is independent of n. Our algorithm can be seen as a modification of the approximation algorithm developed by Aingworth, Motwani, and Oldham (2000) into a randomized algorithm, which improves the accuracy theoretically as well as practically.

7. 全眞嬉, 金子法正,　定兼邦彦, 徳山豪:
“数値データベースに対するエキスパート付き決定木の構築”, FIT2004 第 3 回情報科学技術フォーラム, F-50, 331-332, 2004 年 9 月.
概要: 予測精度の高い決定木を構築するための手法の提案を行う．決定木を構成する際の問題点として過学習がある．学習データに対する最適な決定木と未知データに対する予測精度にはトレードオフが生じるため，決定木の枝刈りが必要となる．　本論文では分割時の誤差をより小さくするために，数値データを最適ピラミッド近似を利用して整理し，構築されたピラミッドをエキスパートとして用いた，個々のデータに依存する柔軟な枝刈り手法を提案した．

8. 丸山謙志, 王冠超, 徳山　豪:
“Web 検索解析によるクラスタリング手法の研究 ”, FIT2004 第 3 回情報科学技術フォーラム, D-43, 99-100, 2004 年 9 月.
概要: WEB 検索におけるクラスタリングで、ラベルクラスタの精密化をネットワークフローを用いて行い、従来より利用しやすいクラスタリングシステムを試作した

9. 丸山謙志, 王冠超, 徳山　豪:
“Web 検索解析によるクラスタリング手法の研究 ”, 第四回データマイニングワークショップ, 29, 55-56, 2004 年 9 月.
概要: 同上

学会大会等

1. 塩浦 昭義:
“二項モデル上でのヨーロピアン・アジアンオプションの価格付けに対する精度保証付き近似解法”, 日本オペレーションズ・リサーチ学会アルゴリズム研究部会, 2004 年 11 月.

2. A. Shioura, T. Tokuyama:
“Ultimate Implementation and Analysis of the AMO Algorithm for Pricing European-Asian Options”, Workshop on New Horizons in Computing, 2005 年 3 月.

3. J. Chun，K. Sadakane，T. Tokuyama:
“Construction of Expert Guided Decision Tree on Numeric Database”, The 2nd

Student-Organizing Int'l Mini-Conference on Information Electronics System, 241-244, 2004 年 10 月.

4. 全眞嬉，徳山豪:
“数値データに対するデータマイニング”, 日本オペレーションズ・リサーチ学会第 9 回 SAOR 研究会, 2004 年 5 月.

5. 鈴木晶子，徳山豪:
“データマイニングにおけるクラスタリング”, 日本オペレーションズ・リサーチ学会第 9 回 SAOR 研究会, 2004 年 5 月.

6. 徳山豪:
“計算理論の先端的手法による実用分野開拓– データマイニングを例にして”, 電子情報通信学会 2005 年総合大会、情報システムソサイエティ企画 “計算限界の中心で解法を叫ぶ ” チュートリアル講演, 2005 年 3 月.

A03: 論理関数表現のモデルとシンボリックアルゴリズム

武永 康彦

電気通信大学 電気通信学部 情報工学科
〒 182-8585 調布市調布ヶ丘 1-5-1
takenaga@cs.uec.ac.jp

1 はじめに

分岐プログラムは有向グラフによる論理関数の表現法であり、古くから主に理論的研究が行われていた。近年になって、分岐プログラムに強い制限を加えた二分決定グラフ（OBDD：Ordered Binary Decision Diagram）と呼ばれる表現法が注目され、論理設計支援などの分野で論理関数の内部表現として多く用いられている。そのため、二分決定グラフや、それに類したいくつものモデルについて、論理関数の処理手法やその計算複雑さについて、理論・応用の両面から研究が盛んに行なわれるようになった。

二分決定グラフを用いたアルゴリズムは、基本的に、問題をすべて符号化して論理関数の形で表現し、二分決定グラフ上で論理関数処理を行うことによって問題を解くという形をとっている。このようなアルゴリズムはシンボリックアルゴリズムと呼ばれ、最近では、その実用性から従来広く利用されてきた論理設計支援の分野だけでなく、グラフアルゴリズムなどにおいてアルゴリズム理論の立場からも興味深いシンボリックアルゴリズムの研究が行われるようになりつつある。

本研究では、第一に、シンボリックアルゴリズムに関して、アルゴリズムの入力となる二分決定グラフやそれに類する論理関数表現による様々な問題の表現方法、具体的なアルゴリズムの設計と、その評価方法に関する研究を行なう。具体的な対象としては、まずはグラフ問題を中心に扱う。

シンボリックアルゴリズムは、入力データ（グラフ問題の場合はグラフ）が二分決定グラフなどの形で与えられるという設定のもとでのアルゴリズムであるため、入力を効率よく小さなサイズで表現する論理関数表現のモデルや、効率よく表現できる対象についても研究を行うことが重要である。また、入力のサイズが二分決定グラフのサイズとなるため、二分決定グラフに対するいくつかの基本的操作が一般には指数時間を要する場合がある。そのため、シンボリックアルゴリズムの計算時間の理論的評価方法は、他の多くのモデルの場合と異なっている。現在用いられている評価方法が、理論的・実際的にみてどれほど妥当かについても検討する必要があると考えられる。また、これらの研究成果をもとに、具体的なシンボリックグラフアルゴリズム、それに関連する一般的なグラフアルゴリズムの設計も行なう。

第二に、分岐プログラムや二分決定グラフなど、グラフによる論理関数の表現の基本的性質や複雑さに関する研究、論理関数のグラフ表現と他の表現との関連など、論理関数やその表現法そのものに関する研究を行なう。論理関数表現の基本的性質や複雑さに関する研究は、前述の入力データの二分決定グラフ表現の研究と密接に関連しており、その表現の複雑さを中心に研究を進める。また、グラフ表現と他の表現との関連については、論理関数の主項と二分木表現との対応をもとに定義された正論理関数のクラスである、tree-shellable 論理関数を定義しその性質に関する研究を行なっており、さらに研究を進める。

本年度は、具体的には以下の研究を行なった。まず、二分決定グラフによるグラフの表現およびシンボリックアルゴリズムに関する研究として、区間グラフの区間表現に基づく効率的な二分決定グラフ表現の方法を提案し、その上での基本的なグラフ操作のシンボリックアルゴリズムの設計・評価を行なった。また、基本的グラフ問題のアルゴリズムに関する研究として、比較可能グラフに k 本の辺を加えた、比較可能$+ke$ グラフの頂点彩色問題に対するアルゴリズム、計算量について研究を行ない、k が 1 の場合のみ効率的なアルゴリ

ズムが存在することを示した。

グラフによる論理関数の表現については、非冗長な積和形論理式で与えられた正論理関数が(ordered) tree-shellable 論理関数であるか否かの判定問題について研究を行なった。まず、長さ3以上の項が2個以下の場合の、ordered tree-shellable 関数の判定問題を考え、多項式時間で解ける場合があることを示した。また、各リテラルの出現回数が定数でおさえられる場合には、tree-shellable であるかどうかの判定問題が、多項式時間で解けることを示した。

以下の各章で、これらの研究成果について説明を行なう。

2 区間グラフの二分決定グラフ表現

2.1 概論

二分決定グラフ（Ordered Binary Decision Diagram : OBDD) [1] とは論理関数を表現する有向非巡回グラフである。変数でラベル付けされた内部節点と、論理値でラベル付けされた終端節点を持ち、内部節点は0枝、1枝の2つの出枝を持つ。変数の全順序関係が存在し、根から終端節点への全てのパスにおいて現れる変数の順序がその全順序に従う。変数に値を割り振り、根から変数の値に従って0枝または1枝を辿り、到達した終端節点のラベルが関数の値となる。OBDD から冗長、等価な節点をすべて削除したものを既約な OBDD と呼ぶ。既約な OBDD は、変数の全順序を定めると論理関数の表現が一意に定まる、多くの実用的な関数が比較的小さなサイズで表現できる、論理演算・等価性判定・充足可能性判定など、論理関数に対する基本的処理が高速に行なえる、といった特長を持つ。そのため、論理関数や各種データの表現法として広く用いられ、グラフの OBDD 表現に基づくグラフアルゴリズムの研究も行なわれている [2]。

本研究では、区間グラフの区間表現に基づく OBDD 表現を提案し、その表現の上での基本的なグラフ操作のシンボリックアルゴリズムを示す。

Definition 1 区間グラフ *[3]* とは、数直線上の区間の集合を $I = \{K_1, K_2, \cdots, K_n\}$ としたとき、

1. 各区間 $K_1, K_2, \cdots, K_n$ に対応させて頂点を $V = \{K_1, K_2, \cdots, K_n\}$ とする、
2. K_i と K_j が共通する区間をもつ時、$(K_i, K_j) \in E$ とする、

という形で表せるグラフである。区間 K_i の最小値を a、最大値を b とした時、$K_i = [a, b]$ と表す。また、区間集合 I を区間グラフの区間表現という。

区間グラフは実際的な応用範囲も広く、重要なグラフクラスのひとつとして広く研究が行なわれている。

また、区間同士に包含関係がない区間表現から出来る区間グラフを proper 区間グラフという。Proper 区間グラフでは区間の長さを一定に変換する事が出来る。

基本的グラフ操作としては、頂点に隣接する頂点集合を求める、頂点集合に隣接する頂点集合を求める、頂点からある距離以内にある頂点集合を求める、という操作を考える。後の 2 つの操作は入力の OBDD サイズに対し、最悪で指数時間がかかることが知られている。しかし、一般的な OBDD 表現を用いた場合との比較のため、またどの程度の大きさのグラフを扱えるかを把握するため、区間グラフの頂点数を基準にした計算量の評価を行っている。

2.2 区間表現に基づく OBDD 表現

一般にグラフを OBDD で表現する場合、頂点を2進数で符号化し、頂点対が辺を持つ場合のみ1となる関数を OBDD で表す。それに対し、区間グラフではその区間表現に基づいて OBDD で表現することも可能である。本章では、区間表現に基づく OBDD の表現方法を示す。

- 区間の両端の値を s ビットの2進数で表し、辺を $2s$ ビットで符号化する。
- 区間の左端、右端を符号化したものをそれぞれ x、y とし、その特性関数 $\chi_I(x_1, x_2, \cdots, x_s, y_1, y_2, \cdots, y_s)$ を OBDD で表す。変数順序は $x_1, x_2, \cdots, x_s, y_1, y_2, \cdots, y_s$ の順とする。つまり、$[x, y]$ が区間集合の一要素と一致していれば1を返す OBDD を作成する。

図 2.1 に区間グラフの区間表現とその OBDD 表現の例を示す。

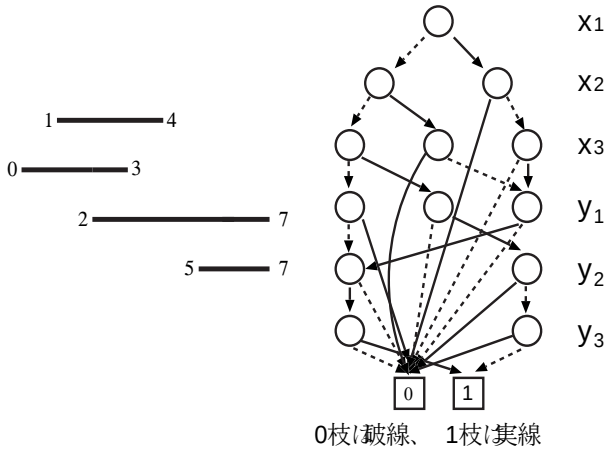


図 2.1: 区間グラフの区間表現 (左) と OBDD 表現 (右)

区間表現において、グラフに変化を与えない範囲で区間を短くする事が出来る。したがって、区間表現では扱う区間の端点を $0 \sim 2n-1$ の整数で表せる。このように表した場合、χ_I の OBDD の高さは $2\lceil \log 2n \rceil$、幅は最大で n になる。よってサイズについては $O(n \log n)$ となる。一般的な表現法を用いた場合のサイズは、辺の数を m とすると、$O(m \log n)$ となり、区間表現に基づいた表現の方がサイズが小さくなる。

また、proper 区間グラフの場合、区間の長さが一定の場合、区間の片側の端の値が決まればもう片側の値も決まる。したがって、片側の端点のみで χ_I の OBDD 表現が出来る。この時、扱う区間の端点は、区間の長さを l とすると、$0 \sim ln$ 以内に収まる。$1 \leq l \leq n$ であるので、扱う区間の大きさは $O(n^2)$ となる。Proper 区間グラフの χ_I を片側の端点で表した場合、一般の区間グラフの場合と同様に、サイズは $O(n \log n)$ となる。

2.3 区間グラフ上でのアルゴリズム

区間に隣接する区間集合を求めるアルゴリズム

χ_I の OBDD から区間 $[a,b]$ に隣接しない区間を取り除くことにより求める区間集合を得る事を考える。区間 $[a,b]$ に隣接しない区間 $[x,y]$ の条件とは $x < b$ または $y > a$ を満たす事である。以下にアルゴリズムを示す。

1. x, y が $x < b$ または $y > a$ をみたすときに 0 を返す OBDD を作成する。
2. 1 で得られた OBDD と χ_I の OBDD の AND をとる。
3. 2 で得られた OBDD と区間 $[a,b]$ の OBDD との排他的論理和をとり，得られた OBDD が求める区間集合を表す。

1,2 の操作により区間 $[a,b]$ に隣接しない区間を取り除くことが出来る。このアルゴリズムの計算量は $O(n \log^2 n)$ となる。

これをもとに、区間集合に隣接する区間集合を求める操作は区間集合に含まれる区間数を k とすると、$O(kn^2 \log^2 n)$ 時間で実行できる。

頂点から距離 l 以内にある頂点集合を求めるアルゴリズム

ある区間 $[a,b]$ から距離 1 以内の区間集合 I_1 に含まれる区間 $[x_i, y_i]$ のうち、端点の最小値 x_{min} と最大値 y_{max} の間にある点は必ず区間集合 I_1 に含まれる。よって、区間集合 I_1 に隣接する区間集合 I_2 を求める事は、区間 $[x_{min}, y_{max}]$ に隣接する区間集合を求める事と同じである。この操作を繰り返すことにより、距離 l 以内にある頂点集合を求めることができる。この計算量は $O(ln \log^2 n)$ となり、一般的なグラフの OBDD 表現を用いた場合より効率的に実行できる。

3 比較可能+ke グラフの彩色問題

3.1 概論

一般の入力に対して NP 完全である問題への取り組みの 1 つとして, 問題の入力の一部をパラメータとして特定の値 k に固定して, 特定の k の値の元では容易に解けるかどうかを考える方法がある.

本研究では、グラフの頂点彩色問題を扱う。頂点彩色問題は次で定義される.

Input: グラフ $G = (V, E)$, 正の整数 $t \leq |V|$

Question: G は t 彩色可能か. つまり, すべての G の辺 (u,v) に対して, $f(u) \neq f(v)$ を満たす関数 $f : V \to \{1,2,\ldots,t\}$ が存在するか.

t 彩色可能である t のうち最小のものを彩色数 $\chi(G)$ という. 頂点彩色問題は彩色数を 3 に固定したところで NP 完全である.

しかし、特定の性質を持つグラフだけを対象とした場合には、頂点彩色問題が多項式時間で解けることがある。比較可能グラフ [3] もそのような性質を持つグラフクラスのひとつである [5]. グラフ G が比較可能グラフであるとは, G の各無向辺を適当な方向の有向辺にしたときに, そのグラフが推移的グラフになるものが存在するときをいう. ただし, 推移的グラフとは辺 (u,v), (v,w) が存在するならば辺 (u,w) も存在するような有向グラフのことである. このとき, 比較可能グラフに「ある程度近い」グラフについても多項式時間で解ける可能性がある.

このように、あるグラフ族に近いグラフとして、ここでは以下のようなグラフ族を考える。$\mathcal{F}$ をあるグラフ族とすると, $\mathcal{F}$ グラフに辺を k 本加えたグラフからなるグラフ族を $\mathcal{F}$+ke グラフと呼ぶ. また同様に, $\mathcal{F}$ グラフから辺を k 本取り除いたグラフからなるグラフ族を $\mathcal{F}$-ke グラフと呼ぶ. $\mathcal{F}+ke$ グラフ $G=(V,E)$ のモジュレータとは, $G-E_k \in \mathcal{F}, |E_k| \leq k$ となるような $E_K(\subset E)$ のことである. つまり, $\mathcal{F}$+ke グラフからモジュレータに含まれる辺を取り除くと $\mathcal{F}$ グラフが得られる.

本研究では, k を入力のパラメータとし, k の値を固定したときに比較可能+ke グラフの頂点彩色問題の計算量がどのように変化するかを調べる. まず、比較可能+1e グラフの頂点彩色問題は $O(\gamma|E|)$ 時間で解くことができることを示す. ただし γ は頂点の最大次数である. 次に, 3SAT 問題から比較可能+2e グラフの頂点彩色問題への帰着を示し, 比較可能+2e グラフの頂点彩色問題は NP 完全であることを証明する.

関連研究として二部グラフに辺を k 本加えた二部+ke グラフに対する頂点彩色問題の研究がある [4]. 二部+2e グラフの彩色問題は多項式時間で解ける. しかし二部+3e グラフに対しては NP 完全である. 比較可能グラフは二部グラフを含むので, この結果から比較可能+3e グラフの頂点彩色問題は NP 完全であることが分かる. この他, 二部グラフに 1 個の頂点とその頂点に接続する辺を任意に加えた二部+1v グラフに対しては多項式時間, また同様に二部+2v グラフに対しては NP 完全であることが分かっている.

3.2 比較可能+1e グラフの彩色問題

グラフ G のクリーク数 $\omega(G)$ とは, G の完全部分グラフのうち最大のものの位数である. 比較可能グラフは理想グラフであり、 クリーク数と彩色数が等しい. 比較可能グラフのクリーク数および彩色数は多項式時間で求められる. 推移的グラフ $G=(V,E)$ の頂点 u,v について, u が v へ隣接しているとき $f(u) < f(v)$ を満たすような関数 $f : V \to \{1,2,\ldots,\omega(G)\}$ を, G のレベル付けといい, このとき $f(u)$ を u のレベルという. 同じレベルの頂点を同じ色で彩色すれば、$\omega(G)$ 色での頂点彩色が得られる。

比較可能+1e グラフを G, G のモジュレータを $E_1((a,b) \in E_1)$ とすると, $G' = G - E_1$ は比較可能グラフとなる. なお, ここではモジュレータはあらかじめ与えられているものとする. もし仮にモジュレータが未知であったとしても, 比較可能グラフの判定は多項式時間でできるので, モジュレータを探すことは多項式時間でできる.

比較可能+1e グラフ G の彩色数 $\chi(G)$ は少なくとも $\chi(G')$, また高々 $\chi(G')+1$ である. G' における彩色のうち頂点 a,b が互いに異なる色で彩色されるものはそのまま G の彩色となり, 頂点 a,b がともに同じ色で彩色されるものはそのままでは G の彩色として不適切である. そこで, G における $\chi(G)$ 彩色において, 頂点 a,b を互いに異なる色で彩色できる条件として, 以下の補題を示す.

Lemma 1 *レベル l の 2 つの頂点 a,b を異なる色で彩色できる必要十分条件は, レベル $l-1$ と l の頂点から誘導される部分グラフ, およびレベル l と $l+1$ の頂点から誘導される部分グラフの少なくともどちらか一方において a,b が連結でないことである.*

この補題の条件を満たすかどうかを判定するアルゴリズムの時間計算量は、比較可能グラフ G'

の推移的グラフを求める時間に依存し、$O(\gamma|E|)$ となる。ただし, γ は頂点の次数の最大値である.

Theorem 1 比較可能*+1e* グラフの彩色問題は $O(\gamma|E|)$ 時間で解くことができる. ただし γ は頂点の次数の最大値である.

3.3 比較可能+2e グラフの彩色問題

比較可能+2e グラフを G, G のモジュレータを E_2 としたとき, G の彩色数 $\chi(G)$ は少なくとも $\chi(G-E_2)$ であり, また高々 $\chi(G-E_2)+2$ である.

比較可能+2e グラフ G の頂点彩色問題の 2 つのパターンとして $\chi(G-E_2)$ 色彩色問題と $\chi(G-E_2)+1$ 色彩色問題の NP 完全性を示す. 以下の 2 つの定理は、ともに 3SAT からの帰着により証明される。

Theorem 2 比較可能*+2e* グラフ G の $\chi(G-E_2)$ 色彩色問題は *NP* 完全である.

Theorem 3 比較可能*+2e* グラフ G の $\chi(G-E_2)+1$ 色彩色問題は *NP* 完全である.

また, 定理 2 および定理 3 のどちらからでも, 次の系が導かれる.

Corollary 1 比較可能*+ke* グラフの頂点彩色問題は $k \geq 2$ のとき *NP* 完全である.

4 Tree-Shellable 論理関数の判定問題

4.1 概論

論理関数の特性を理解し，明らかにすることは，計算機科学の様々な分野において重要なことである．積和形論理式 (Disjunctive Normal Form Boolean Formula：DNF) は，論理関数の代表的な表現法の 1 つである．それぞれの積項は論理関数の内項 (implicant) に相当し，特に主項 (prime implicant) は，論理関数の最小形を表すなど，非常に重要な概念である．特に、正論理関数は非冗長な積和形正論理式 (Positive DNF：PDNF) により一意に表現される。一方、二分決定木も論理関数のグラフによる表現法として広く用いられている。

Tree-shellable 論理関数 [6] とは，正論理関数において関数の主項とその関数を表す二分決定木の 1 ノードへたどるパスの数が等しい論理関数である．また、Ordered tree-shellable 論理関数は tree-shellable 論理関数の一種であり，関数を表す二分決定木が順序付き二分決定木となっているものである．論理関数 f が (oedered) tree-shellable であれば，f の双対関数 f^d を求めるのは容易であり，f の DNF 表現から f^d の非冗長な DNF 表現を多項式時間で求めることが可能である．また、各変数が 1 となる確率が与えられたとき、$f=1$ となる確率を求める問題はある種のシステムの信頼性計算に対応しており、f が shellable であれば、この問題も容易に解くことができる。

本研究では、正論理関数が積和形論理式で与えられたとき、その関数が tree-shellable あるいは、ordered tree-shellable であるかどうかを判定する問題の計算複雑さについて考察する。これまでに、ordered tree-shellable 関数の判定問題は一般に NP 完全であることが明らかにされている [7]。また、各積項のリテラル数が 2 となる quadratic 論理関数の場合は、ともに多項式時間で判定可能となる。さらに、各積項の長さが定数で抑えられる場合には tree-shellable 関数の判定が多項式時間で可能であることも示されている。本研究では、どのような関数であれば多項式時間で判定可能であるかを明らかにすることを目的に研究を進める。

4.2 Tree-Shellable 論理関数

二分決定木は論理関数を表す，ラベル付けされた木である．二分決定木の根ノードから値が 1 である葉ノードまでのパスを 1 パスと呼ぶ．特に、変数の全順序 π が存在し，二分木の全てのパスにおいて，現れる変数の順序が π に矛盾なく従っている場合，その二分木を順序付き二分決定木という．π を順序付き二分決定木の変数順序と呼ぶ.

Definition 2 [6] f は *PDNF* $f=\bigvee_{k=1}^{m}\bigwedge_{i\in I_k} x_i$ で表されているとする．f を表す *(*順序付き*)* 二分決定木で m 個の *1* パスを持つものが存在するとき,

f は *(Ordered) tree-shellable* であるという．f を表す変数順序 π の順序付き二分決定木で m 個の *1* パスを持つものが存在するとき，f は π のもとで *ordered tree-shellable* であるという．

図 2.2 に例を示す。(a) は f が (ordered) tree-shellable であることを示している。(b) の二分決定木は g の積項数より多い 1 パスを持っている。g を表す二分決定木は必ず積項数より多い 1 パスを持つため、g は tree-shellable ではない。

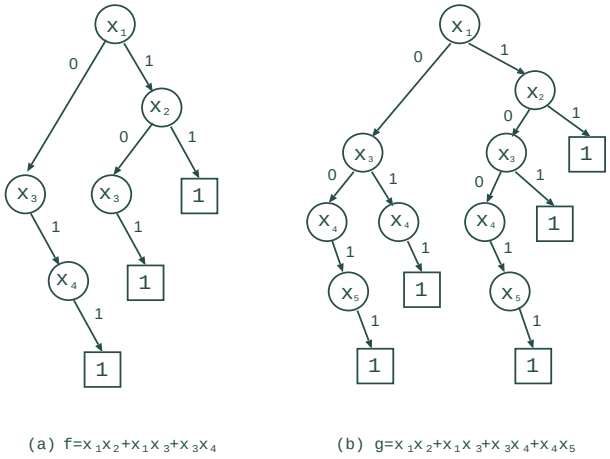


図 2.2: Tree-Shellable 関数と Tree-Shellable でない関数

Theorem 4 *[6]* $f = \bigvee_{k=1}^{m} \bigwedge_{i \in I_k} x_i$ が *tree-shellable* であるとき，以下を満たす二分決定木 T を構成できる．

1. T は $P_1, \cdots, P_m$ の m 個の *1* パスを持つ．

2. 各々の $P_k (1 \leq k \leq m)$ は $i \in I_k \leftrightarrow x_i \in P_k$ を満たす項 I_k に対応する．

4.3 Quadratic 関数に積項を加えた場合の判定複雑さ

Quadratic 関数については、tree-shellable と ordered tree-shellable は等価になり、多項式時間で判定が可能である。これは、quadratic 関数の変数を頂点、積項を辺として表したグラフが cotriangulated グラフとなることと、その関数が (ordered) tree-shellable であることが等価であることより示される。

本章では、リテラル数 3 以上の項を高々2 個持つ場合の ordered tree-shellable 関数の判定複雑さを考える。

まず、リテラル数 3 以上の項を 1 個のみ持つ場合を考える。この形の関数 F を、$K = x_{k_1} x_{k_2} \cdots x_{k_m}$ を長さ 3 以上の項とし、$F = f_q + K$ と表す。f_q を表すグラフ G において，K という頂点をあらたに追加する．K は，$x_{k_1}, x_{k_2}, \cdots, x_{k_m}$ が辺を持つ頂点全てと辺を持つものとする．このグラフを $f_q + K$ を表すグラフと言い，G_K とする．

Theorem 5 F が *ordered tree-shellable* である必要十分条件は，グラフ G_K が *cotriangulated* グラフであり，かつグラフ G_K において K が *cosimplicial* ノードであることである．

この定理により、リテラル数 3 以上の主項が高々 1 個の場合は多項式時間で判定可能であることがわかる。また、リテラル数 3 以上の主項が 2 個以上の場合については、次の結果が示される。

Theorem 6 リテラル数が *3* の主項が *2* 個、それ以外の主項はリテラル数 *2* 以下の関数については、多項式時間で *ordered tree-shellable* 関数の判定が可能である。

4.4 リテラルの出現回数に制限を加えた場合の判定複雑さ

本章では、リテラルの出現回数に制限を加えた tree-shellable 論理関数の判定複雑さについて考える。

Theorem 7 各リテラルの出現回数が高々 i 回の *PDNF* で表される論理関数 f で、f の積項にリテラル数 *2* 以上の積項が $i^2 + 1$ 個以上あるものは *tree-shellable* とはならない。

これにより、各リテラルの出現回数が定数であれば、tree-shellable となる関数の積項数も定数で抑えられることがわかる。したがって、次のような簡単なアルゴリズムにより、多項式時間で tree-shellable であるかどうかが判定可能となる。

1. 全ての変数に対して順に以下を行う。ひとつでも tree-shellable になるものがあればよい。

2. 選ばれた変数を根の変数とし、その変数を含む積項を右部分木側、含まない積項を左部分木側のパスとする。この組合せが tree-shellable 論理関数の条件にあうかを確認する。

3. 右部分木側、左部分木側の関数が tree-shellable になるか、再帰的に調べ、
ともに tree-shellable となれば、元の関数も tree-shellable である。

参考文献

[1] R.E. Bryant, *Graph-Based Algorithms for Boolean Function Manipulation*, IEEE Trans. Comput. Vol.C-35, No.8, 1986.

[2] R. Gentilini and A. Policriti, *Biconnectivity on Symbolically Represented Graphs: a Linear Solution*, Proc. 14th ISSAC 2003.

[3] M.C. Golumbic, *Algorithmic Graph Theory and Perfect Graphs 2nd Ed.*, Elsevier, 2004.

[4] Leizhen Cai, "Parameterized Complexity of Vertex Colouring", Discrete Applied Mathematics, 127, No.3, 415-429, 2003.

[5] Grotschel, M., Lovasz, L. and Schrijver, A., "Polynomial Algorithms for Perfect Graphs.", Annals of Discrete Mathematics, 21, 325-356, 1984.

[6] Y. Takenaga, K. Nakajima and S. Yajima, Tree-Shellability of Boolean Functions, Theoret. Comput. Sci. 262, 633-647, 2001.

[7] E. Boros, Y. Crama, O. Ekin, P. L. Hammer, T. Ibaraki and A. Kogan, Boolean Normal Forms, Shellability and Reliability Computations, SIAM J. Discrete Mathematics, vol.13, no.2, 212-226, 2000.

研究業績一覧

学術論文

1. 東海林貴司, 武永康彦:
"積項の長さに制限を付けた論理関数の Ordered Tree-Shellability", 京都大学数理解析研究所講究録, 1375, 130–136, 2004 年 5 月.
概要: Ordered tree-shellable 論理関数とは、1 へのパスの個数が主項の数と同じになるような順序付き二分木表現を持つ正論理関数である。本論文では、積和形論理式で与えられた関数が ordered tree-shellable であるか否かを判定する問題を考える。各積項の長さが 2 以下の場合は多項式時間で判定できることが知られているが、長さ 3 以上の積項を 1 個含む場合、長さ 3 の積項を 2 個含む場合も多項式時間で判定できることを示す。

2. 東出賢一, 武永康彦:
"比較可能+ke グラフの彩色問題", 京都大学数理解析研究所講究録, (掲載予定).
概要: 一般には NP 完全である頂点彩色問題は、比較可能グラフに対しては多項式時間で解くことができる。そのため、比較可能グラフに近いグラフについても多項式時間で解ける可能性がある。本論文では、比較可能グラフに辺を k 本加えた比較可能 $+ke$ グラフを考える。まず、比較可能 $+1e$ グラフの彩色問題が多項式時間で解けることを示す。次に、3SAT 問題からの帰着により、比較可能 $+2e$ グラフの彩色問題が NP 完全であることを示す。

研究会等

1. 東出賢一, 武永康彦:
"比較可能+ke グラフの彩色問題の計算量", 電子情報通信学会技術研究報告, COMP2004-82, 71–77, 2005 年 3 月.
概要: 比較可能 $+ke$ グラフとは、比較可能グラフに辺を k 本加えたグラフである。本論文では、k を定数としたときの比較可能 $+ke$ グラフの頂点彩色問題の計算量を考える。まず、比較可能 $+1e$ グラフの彩色問題が多項式

時間で解けることを示す。次に、3SAT 問題から比較可能 $+2e$ グラフの彩色問題への多項式時間帰着を示し、比較可能 $+2e$ グラフの彩色問題が NP 完全であることを示す。

2. 加藤木直, 武永康彦:
“リテラルの出現回数に制限を加えた関数の tree-shellablity 判定問題”, 電子情報通信学会技術研究報告, （発表予定）.
概要: Tree-shellable 論理関数とは、1 へのパスの個数が主項の数と同じになるような順序付き二分木表現を持つ正論理関数である。同一リテラルの出現回数が高々定数回に制限された正の積和形論理式が与えられたときに、それが tree-shellable であるかどうかを多項式時間で判定できることを示す。

学会大会等

1. 松川弘明, 武永康彦:
“区間グラフの OBDD 表現について”, 2005 年電子情報通信学会総合大会, D-1-9, 2005 年 3 月.

A04: 組み合わせ最適化における指数サイズ・多項式時間近傍の設計

玉木　久夫　　井口　幸洋

明治大学　理工学部　情報科学科
〒２１４－８５１７ 川崎市多摩区東三田１－１－１
{tamaki,iguchi}@cs.meiji.ac.jp

1　はじめに

本課題では、組み合わせ最適化問題に対する指数サイズの近傍のアプローチをテーマにしている。おもに、次の３つの方向から研究を進めている。

(A) 一般的、基礎的な技法およびそのための理論

(B) 具体的な問題に対する近傍と解法の設計と実装

(C) 解法のハードウェア化ないし準ハードウェア化

(A) において、技法の核にあるのは、グラフやハイパーグラフの再帰的分割であり、幅の小さい木分割 [5, 6] や分枝分割 [7] を効率的に求めることが重要になる。特にこの研究では、実装のしやすい動的計画法の基礎となる分枝分割を多用している。一般のグラフの場合には、最適の木分割や分枝分割を求める問題はＮＰ困難であるが、平面グラフの場合には、分枝分割を求める $O(n^4)$ 時間のアルゴリズムが知られていた [8]。今年度は、海外研究協力者である Qiangping Gu と共にこの計算時間を $O(n^3)$ に改良することに成功した。その技術的な詳細については 2 節で述べる。

(B) においては、巡回セールスマン問題、メッシュ最適化問題に対して具体的な研究を行い、クリーク被覆、集合被覆問題などの被覆系統の問題に対して予備的な検討を行った。巡回セールスマン問題については、これまでに追求して来たグラフ分割に基づくアプローチをいったん休止して、文献にあるさまざまな指数サイズ近傍の実験を行った。（ピラミッド近傍、マッチング近傍、Ballas-Simonetti 近傍など）。その結果、近傍の大きさと、それによって得られる局所最適解の良さには直接の関係がないことが再確認された。いずれも方法も、他の代表的な発見的解法に劣る結果となっており、近傍の設計手法の重要さを再認識した。質の良い近傍を設計するためには、問題のグラフ構造を利用する必要があることを再確認し、ふたたびグラフ分割に基づくアプローチへ戻ることになった。メッシュ最適化については、グラフ分割に基づいた一般的な近傍の設計を行い、それをメッシュ最適化を単純化したグラフ描画問題と、地形図の簡略化問題に適用して実験を行った。その技術的概要については 3 節で述べる。

(C) については、予備的な考察と使用する技法についてＦＰＧＡを中心にさまざまな研究を行った。その技術的概要については 4 節で述べる。

2　平面グラフ最適分枝分割の $O(n^3)$ 時間アルゴリズム

G を無向グラフとする。G の分枝分割とは、G の辺集合を葉の集合として持つ、内点の次数がいずれも 3 であるような木のことを言う。T が G の分枝分割であるとき、その各辺 $\{p, q\}$ に対して $L_T(p, q) \subseteq E(G)$ によって p から q を通らない T の道によって到達できる T のすべての葉からなる集合を表す。T における G に関する $\{p, q\}$ の幅を、$L_T(p, q))$ の辺と $L_T(q, p))$ の辺の両方に接続するような G の頂点の個数と定義する。G の分枝分割 T の幅は、その辺の G に関する幅の最大値と定義される。G の分枝幅は、G の分枝分割の幅の最小値と定義される。

分枝幅は Robertson と Seymour [7] によってよりよく知られた木幅の概念 [5, 6] との関連にお

いて導入された。分枝幅や木幅の小さいグラフにおいては、動的計画法によりさまざまな組み合わせ問題を効率よく解くことができるため、グラフの分枝幅・木幅を決定したり、最小幅の分割を求めたりする問題は極めて重要である。分枝幅や木幅が定数で抑えられる場合には、これらの問題はいずれも線型時間で解くことができる [3]。しかしながら、与えられたグラフの幅が k を超えないかどうか決定する問題は、k が入力の一分として与えられた場合ＮＰ完全である [1, 8]。グラフを平面グラフに制限した場合には、木幅に対しては依然として多項式時間アルゴリズムが知られていないものの、分枝幅を求める $O(n^2)$ 時間のアルゴリズムが Seymour と Thomas [8] によって与えられている。同じ論文には、この分枝幅アルゴリズムをサブルーチンとして、平面グラフの最適な分枝分割を求める $O(n^4)$ 時間のアルゴリズムが与えられている。我々は、このアルゴリズムの実行時間を $O(n^3)$ に改良した。以下では、その技術的な概要を述べる。

2.1 準備

多重グラフ G に対して、$V(G)$ によってその頂点集合、$E(G)$ によってその辺集合を表す。各頂点集合 $X \subseteq V(G)$ に対して、$\delta_G(X)$ によって、X のなかにひとつの端点をもち、その外にもう一方の端点を持つ辺の集合を表す。互いに素な頂点集合 $U, V \subseteq V(G)$ に対して、$E_G(U,V)$ によって、U のなかにひとつの端点をもち、V の中にもう一方の端点を持つ辺の集合を表す。Seymour と Thomas　の平面グラフに対する分枝幅アルゴリズムおよび分枝分割アルゴリズムの双方は共に関連した多重グラフに対する刻み幅・分割への帰着に基づいている。

多重グラフ G の刻み分割は G の頂点集合を葉の集合として持つ、内点の次数がいずれも 3 であるような木のことを言う。T が G の刻み分割であるとき、その各辺 $\{p,q\}$ に対して $L'_T(p,q) \subseteq V(G)$ によって p から q を通らない T の道によって到達できる T のすべての葉からなる集合を表す。T における G に関する $\{p,q\}$ の幅を、$L'_T(p,q))$ の頂点と $L'_T(q,p))$ の頂点を結ぶような G の辺の個数と定義する。G の刻み分割 T の幅は、その辺の G に関する幅の最大値と定義される。G の刻み幅は、G の刻み分割の幅の最小値と定義される。

G を、描画の指定された平面グラフとする。G のメディアルグラフ $M(G)$ [8] とは、G の平面双対グラフの、頂点集合と面集合の接続 2 部グラフのことを言う。G が単純グラフであっても一般には $M(G)$ は多重グラフになることに注意する。Seymour と Thomas [8] は、$M(G)$ の刻み幅は G の分枝幅のちょうど 2 倍であることを示した。さらに、$M(G)$ の最適刻み分割から G の最適分枝分割への変換は線型時間で行うことができる。そこで、我々は、平面多重分割の最適刻み分割を求めるアルゴリズムを考えることにする。

定理 1 G を n 個の頂点と $O(n)$ 本の辺を持つ平面多重グラフとするとき、G の最小幅刻み分割は $O(n^3)$ 時間で構成することができる。

この結果を証明するために、Seyour と Thomas のアルゴリズムを幾分異なった枠組みで記述する。まず、刻み分割を根付き 2 分木とみなすことから始める。$\sigma(V)$ によって、集合 V の一元部分集合全体からなる集合を表す。集合 V における 2 進併合を次のように帰納的に定義する。

1. $\sigma(V)$ は V における 2 進併合である。
2. もし $\mathcal{M}$ が V における 2 進併合であり、X, Y が $\mathcal{M}$ における V の相異なる極大部分集合であるならば、$\mathcal{M} \cup \{X \cup Y\}$ は V における 2 進併合である。

V における 2 進併合が V 自身を要素として持つとき、その 2 進併合は完全であるという。G をグラフとするとき、$V(G)$ の完全 2 進併合には自明な形で G の刻み分割が対応する。反対に、G の刻み分割が与えられたとき、その分割の辺のひとつを根として選ぶことにより、その刻み分割に対応する $V(G)$ における完全 2 進併合が決定される。$V(G)$ における 2 進併合 $\mathcal{M}$ の幅を $X \in \mathcal{M}$ のすべてを考えたときの $|\delta_G(X)|$ の最大値と定義する。$\mathcal{M}$ が完全であるとき、この定義は $\mathcal{M}$ に対応する刻み分割の幅と一致する。$\mathcal{M}$ と $\mathcal{M}'$ が共に $V(G)$ における 2 進併合であるとき、$\mathcal{M}' \supseteq \mathcal{M}$ であるならば $\mathcal{M}'$ は $\mathcal{M}'$ を拡張すると言う。$\mathcal{M}$ を $V(G)$ における 2 進併合とし、その幅は G の刻み幅 k 以下であるとする。X と Y を $\mathcal{M}$ の相異なる

極大要素とするとき、もし $\mathcal{M} \cup \{X \cup Y\}$ を拡張する完全２進併合で幅が k であるものがあるならば、X と Y は $\mathcal{M}$ において併合可能と言うことにする。

我々は、Seymour と Thomas の平面グラフに対する分枝分割アルゴリズムを、２進併合の概念を用いて次のように定式化する。これ以降 G は常にアルゴリズムに与えられた多重平面グラフを表し、k はその刻み幅を表すものとする。このアルゴリズムは初期２進併合 $\sigma(V(G))$ から出発して、$V(G)$ の完全２進併合が得られるまで２進併合を拡張して行く。その仮定で、「保持している２進併合は、幅 k の２進併合に拡張可能である」という不変条件を保持する。ここで、k は入力グラフ G の刻み幅を表す。

Algorithm ST
入力: 連結な n 頂点、$O(n)$ 辺平面多重グラフ G
出力: $V(G)$ の刻み分割で 幅が最小のもの
(1) G の刻み幅 k を決定する。
(2) $\mathcal{M}^0 = \sigma(V(G))$ とおき、$i = 1$ とおく。
(3) 以下を $i < n$ である間繰り返す。
(3.1) $\mathcal{M}^{i-1}$ の対 $\{X, Y\}$ で、$E_G(X, Y) \neq \emptyset$ であるようなものを、併合可能な対がみつかるまで走査する。併合可能な対 $\{X, Y\}$ がみつかったら、$X^i = X \cup Y$. とおく。
(3.2) $\mathcal{M}^i = \mathcal{M}^{i-1} \cup \{X^i\}$ とおいて、i を $i+1$ におきなおす。
(4) 完全２進併合 $\mathcal{M}^{n-1}$ の表す刻み分割を返す。

このアルゴリズムの正しさは、i についての数学的帰納法によって各 $\mathcal{M}^i$ が定義されかつ幅 k の完全２進併合に拡張可能であることを示すことによって証明される。証明はここでは省略する。

X と Y が $\mathcal{M}$ において併合可能かどうか調べるには、G において $\mathcal{M}' = \mathcal{M} \cup \{X \cup Y\}$ の各要素である頂点集合をそれぞれひとつの頂点に縮約して得られる多重グラフ $G_{\mathcal{M}'}$ に対して Seymour と Thomas の刻み幅アルゴリズムを呼び、その幅が k 以下であるかどうかを調べる。このテストの呼び出し回数は $O(n^2)$ 回であり、刻み幅アルゴリズムの実行時間は $O(n^2)$ であるため、アルゴリズムＳＴの全体の実行時間は $O(n^4)$ となる。

この、刻み幅アルゴリズムを用いた併合可能性のテストを高価なテストと呼ぶ。次のサブセクションでは、高価なテストの回数を減らすための補題を与える。

2.2 バリア補題

補題 1 G を刻み幅 k の多重グラフとする。$\mathcal{M}$ を $V(G)$ における２進併合とし、X, Y を $\mathcal{M}$ の相異なる極大要素とする。X, Y が $X', Y', Z, W \in \mathcal{M}$ を用いて $X = X' \cup Z$、$Y = Y' \cup W$ と表され、かつ $E_G(Z, W) = \emptyset$ であると仮定する。このとき、もし X と Y が $\mathcal{M}$ において併合可能であり $|\delta_G(X' \cup Y')| \leq k$ であるならば X' と Y' は $\mathcal{M} \setminus \{X, Y\}$ において併合可能である。

証明: $\mathcal{M}' = \mathcal{M} \setminus \{X, Y\}$ とおき、また $\mathcal{M}^*$ によって $\mathcal{M} \cup \{X \cup Y\}$ を拡張する幅 k の完全２進併合を表す。$\mathcal{M}_1 = \mathcal{M}' \cup \{X' \cup Y', X' \cup Y' \cup Z\} \cup (\mathcal{M}^* \setminus \mathcal{M})$、$\mathcal{M}_2 = \mathcal{M}' \cup \{X' \cup Y', X' \cup Y' \cup W\} \cup (\mathcal{M}^* \setminus \mathcal{M})$ とおくと、$\mathcal{M}_1$ と $\mathcal{M}_2$ はともに $\mathcal{M}' \cup \{X' \cup Y'\}$ を拡張する $V(G)$ における完全２進併合である。したがって X' と Y' が $\mathcal{M}'$ において併合可能であることを示すためには、, $\mathcal{M}_1$ または $\mathcal{M}_2$ の幅が k であることを示せば良い。$\mathcal{M}_1 \setminus \mathcal{M}^* = \{X' \cup Y', X' \cup Y' \cup Z\}$、$\mathcal{M}_2 \setminus \mathcal{M}^* = \{X' \cup Y', X' \cup Y' \cup W\}$、でありまた仮定より $|\delta_G(X' \cup Y')| \leq k$ であるから、$|\delta_G(X' \cup Y' \cup Z)| \leq k$ または $|\delta_G(X' \cup Y' \cup W)| \leq k$ であることを示せば目的は達せられる。. $A = X' \cup Y'$ および $B = V(G) \setminus (X \cup Y)$ とおこう。仮定より $E_G(Z, W) = \emptyset$ であるから、

$$\begin{aligned} &\delta_G(A \cup Z) \\ &\quad = \quad E_G(A, B) \cup E_G(Z, B) \cup E_G(A, W), \end{aligned}$$

が成り立ち、右辺の集合は互いに素であるから

$$\begin{aligned} &|\delta_G(A \cup Z)| \\ &\quad = \quad |E_G(A, B)| + |E_G(Z, B)| + |E_G(A, W)|, \end{aligned}$$

が成り立つ。同様にして

$$\begin{aligned} &|\delta_G(A \cup W)| \\ &\quad = \quad |E_G(A, B)| + |E_G(W, B)| + |E_G(A, Z)| \\ &|\delta_G(A)| \\ &\quad = \quad |E_G(A, B)| + |E_G(A, Z)| + |E_G(A, W)| \\ &|\delta_G(B)| \\ &\quad = \quad |E_G(A, B)| + |E_G(Z, B)| + |E_G(W, B)|. \end{aligned}$$

が成り立つ。したがって

$$\begin{aligned}&|\delta_G(A\cup Z)|+|\delta_G(A\cup W)|\\ &= 2|E_G(A,B)|+|E_G(Z,B)|+\\ &\quad |E_G(W,B)|+|E_G(A,Z)|+|E_G(A,W)|\\ &= |\delta_G(A)|+|\delta_G(B)|.\end{aligned}$$

が成り立つ。さらに、仮定より $|\delta_G(A)|\leq k$ でありまた X と Y は $\mathcal{M}$ において併合可能であるから $|\delta_G(B)|=|\delta_G(X\cup Y)|\leq k$ である。したがって、

$$|\delta_G(A\cup Z)|+|\delta_G(A\cup W)|\leq 2k$$

である、$|\delta_G(A\cup Z)|\leq k$ か $|\delta_G(A\cup W)|\leq k$ の少なくとも一方が成り立つ。[]

$\mathcal{M}$ を $V(G)$ における 2 進併合とする。M の要素の列 $X_0\supset X_1\supset\ldots\supset X_m$ は、各 X_i（$1\leq i\leq m$）が X_{i-1} の $\mathcal{M}$ における極大真部分集合であるとき、$\mathcal{M}$ における連鎖と呼ばれる。C によって上の連鎖を表すとき、X_0 と X_m はそれぞれ C の極大元、極小元と呼ばれ、$\top C$ および $\bot C$ と表される。連鎖 C が条件 $|\delta_G(\top C\setminus\bot C)|>k$ を満たすとき C はバリアと呼ばれる。ここで k は約束どおり、G の刻み幅を表す。

補題 2 *(バリア補題)* $\mathcal{M}$ を $V(G)$ における幅 k 以下の 2 進併合とし、X, Y を $\mathcal{M}$ において併合可能な極大元の対とする。2 進併合 $\mathcal{M}'\subseteq\mathcal{M}$ とその相異なる極大元 $X'\subseteq X$ と $Y'\subseteq Y$ で、次の条件を満たすものがあったとする。

1. $|\delta(X'\cup Y')|\leq k$
2. $E_G(X\setminus X', Y\setminus Y')=\emptyset$
3. $\top B=X$ かつ $\bot B\supseteq X'$ であるようなバリア B は $\mathcal{M}$ のなかに存在しない
4. $\top B=Y$ かつ $\bot B\supseteq Y'$ であるようなバリア B は $\mathcal{M}$ のなかに存在しない

このとき、X' と Y' は $\mathcal{M}'$ において併合可能である。

証明: $Z=X\setminus X'$、$W=Y\setminus Y'$ とおく。$X_0\supset X_1\supset\ldots\supset X_h$ を極大元 $X_0=X$ と極小元 $X_h=X'$ を持つ $\mathcal{M}$ の連鎖とする。同様に、$Y_0\supset Y_1\supset\ldots\supset Y_j$ を極大元 $Y_0=Y$ と極小元 $Y_j=Y'$ を持つ $\mathcal{M}$ の連鎖とする。$\mathcal{M}_1$ を $\mathcal{M}$ から X_i（$0\leq i<h$）と Y_i（$0\leq i<j$）をすべて除いて得られる $V(G)$ の 2 進併合とする。すると $\mathcal{M}_1$ は $\mathcal{M}'$ を拡張し、$X_i\setminus X_{i+1}$（$0\leq i<h$）のそれぞれと $Y_i\setminus Y_{i+1}$（$0\leq i<j$）のそれぞれは $\mathcal{M}_1$ の極大要素である。この $\mathcal{M}_1$ を次のように拡張して、極大元 X,Y を持ち X の極大真部分集合が X' と Z と、Y の極大真部分集合が Y' と W であるような 2 進併合 $\mathcal{M}_2$ をつくる。まぅ、$\mathcal{M}_1$ に $i=2,\ldots,h$ に対して順次 $X_0\setminus X_i$ を加えて極小元が $X_0\setminus X_1$ で、極大元が $X_0\setminus X_h=Z$ であるような連鎖を導入する。同様にして、極小元が $Y_0\setminus Y_1$ で、極大元が W であるような連鎖を導入し、その結果を $\mathcal{M}_2$ とする。もし $\delta_G(X_0\setminus X_i)>k$ であるなら極大元 X_0 と極小元 X_i を持つ $\mathcal{M}$ の連鎖は仮定に反してバリアであるから、したがって $i=2,\ldots,h$ に対して $\delta_G(X_0\setminus X_i)\leq k$ が成り立つ。同様にして、$i=2,\ldots,j$ に対して $\delta_G(Y_0\setminus Y_i)\leq k$ が成り立つ。したがって、$\mathcal{M}_2$ の幅は k 以下である。$\mathcal{M}_2$ の極大要素の集合は $\mathcal{M}$ のそれと等しいので、X と Y が $\mathcal{M}$ において併合可能であるという仮定からそれらが $\mathcal{M}_2$ においても併合可能であることがわかる。

こうして、$X',Y',Z,W\in\mathcal{M}_2$ が成り立ち、$X=X'\cup Z$ と $Y=Y'\cup W$ は $\mathcal{M}_2$ の極大元で、X と Y は $\mathcal{M}_2$ において併合可能である。しかも、仮定より $E_G(Z,W)=\emptyset$ と $|\delta_G(X'\cup Y')|\leq k.$ が成り立つ。したがって補題 1 を $\mathcal{M}_2$ に適用することができ、X' と Y' は $\mathcal{M}_2\setminus\{X,Y\}$ において併合可能であることが結論される。$\mathcal{M}_2\setminus\{X,Y\}$ は $\mathcal{M}'$ を拡張するので X' と Y' は $\mathcal{M}'$ において併合可能である。[]

2.3 高価なテストの節約

この節では $\mathcal{M}^i, 0\leq i\leq n-1$ によってアルゴリズム ST の G に対する実行において順次構築される $V(G)$ の 2 進併合を表す。我々の併合可能性テスト法を記述するために、次の記法を用いる。T^i によって、実行開始から $\mathcal{M}^i$ が構築される直前までに、併合可能性テストが適用された $\mathcal{M}^i$ の要素対すべてからなる集合を現す。T^i は、アルゴリズム ST における、要素対の走査順を指定すれば、入力グラフ G に対して一意に決まる。T^i の部

分集合で、以下に述べる我々の方法において、高価なテストが適用される要素対の集合を P^i で表す。さらに、Q^i によって、P^i に属する要素対のうち、テストの結果が「併合不能」であったようなものの集合を現す。X, Y を $\mathcal{M}^{n-1}$ の相異なる2要素で $E_G(X,Y) \neq \emptyset$ であるようなものとするとき、$\mu_Y(X)$ によって X の $\mathcal{M}^{n-1}$ に属する部分集合で $E_G(X,Y) = E_G(X',Y)$ を満たすののうち、極小なものを表す。さらに、$Q(X,Y)$ によって、$X \supseteq X' \supseteq \mu_Y(X)$ かつ $Y \supseteq Y' \supseteq \mu_X(Y)$ を満たすような $\{X',Y'\} \in Q^{n-1}$ のすべてからなる集合を表す。$\mu_Y(X)$ と $Q(X,Y)$ は i を $X, Y \in \mathcal{M}^i$ なる最小のインデックスとするとき、$\mathcal{M}^i$ と Q^i から決定可能であるので、X と Y の併合可能性をテストするときにアルゴリズムが使用することが可能である。また、対要素ごとの集合包含関係は集合 $Q(X,Y)$ の全順序になっていることに注意する。

倹約併合可能性テスト

入力： $\mathcal{M}^{i-1}$ の相異なる極大元 X と Y

目的：X と Y が $\mathcal{M}^{i-1}$ において併合可能かどうか答える

(1) もし $|\delta(X \cup Y)| > k$ ならば NO と答える。

(2) そうでなく、もし $Q(X,Y) = \emptyset$ であれば高価なテストを実行しその結果を答える。

(3) そうでなければ、$\{X',Y'\}$ を $Q(X,Y)$ の極大対とする。. もし $\top B = X$ かつ $\bot B \supseteq \quad X'$ であるか、$\top B = Y$ かつ $\bot B \supseteq Y'$ であるようなバリア B が $\mathcal{M}^{i-1}$ のなかに存在すれば NO 答える。そうでなければ, 高価なテストを実行してその結果を答える。

補題 3 上の併合可能性テストは正しい結果を答える。

証明: 答えが NO であるときに、X と Y が実際に併合不可能であることを示せばよい。テストがステップ (1) で終わるときには、これは自明である。テストがステップ (3) で高価なテストをスキップして NO と答える場合を考える。$\{X',Y'\}$ を上の手続きで定義されたものとし、$Z = X \setminus X'$ および $W = Y \setminus Y'$ とおく。$Q(X,Y)$ の定義から、$\delta_G(Z,W) = \emptyset \quad$ が導かれる。したがってバリア補題を $\mathcal{M} = \mathcal{M}^{i-1}$ および、$\mathcal{M}'$ を X' と Y' を要素として持つ $\mathcal{M}_j$ で j が最小のものに置き換えて適用することができ、X, Y が $\mathcal{M}^{i-1}$ において併合可能でないことが結論される。[]

補題 4 上の併合可能性テスト法を用いてアルゴリズム ST を実行したとき高価なテストの呼ばれる回数は $O(n)$ である。

証明: 省略。[]

併合可能性テスト以外の部分の計算時間は素朴なデータ表現とアルゴリズムによって $O(n^3)$ に抑えることができる。したがって、定理 1 が成り立つ。

3 メッシュ最適化への巨大近傍アプローチ

以下で述べるアプローチは、三角形メッシュ以外にも適用可能であるが今のところ対象を三角形メッシュにしぼって検討している。メッシュ最適化の最適化基準については、目的に応じてさまざまなものが考えられる。我々のアプローチは、かなり広い範囲の最適化基準に適用可能であるが、これまで実際に適用したのは下で述べる範囲にとどまる。また、メッシュの最適化は、位相構造を固定して頂点の座標だけを変数とする場合と、位相構造も可変とする場合とがあり、将来は後者も扱う予定であるが、現在は前者のみを扱っている。

与えられたメッシュに対する我々の近傍は、そのメッシュにおいて頂点を微小距離動かすことにより得られる。各頂点に対して、移動先の候補（例えば2次元ならば前後左右の単位距離移動と移動せずの合わせて5通り）を定める。理想的には、すべての頂点を独立に動かすことを許す。先の例の場合、頂点数を n とすると近傍の大きさは n^5 となる。メッシュをグラフと見たときの分枝幅が十分小さければ（例えば6以内）であれば、この近傍内の最適解は動的計画法により高速に求めることができる。（ただし、目的関数は部分の最適値から全体の最適値を合成できるための一定の性質を満たすことが条件である。） 分枝幅が大きすぎる場合には、グラフの縮約の技法を用いる。いくつかの頂点集合を選び、そのそれぞれをひとつの頂点に縮約する。縮約された頂点集合においては、各頂点が同一の動きをするという制約を設

けた近傍のなかでの最適解は、縮約結果のグラフの分割に基づいた動的計画法により求めることができる。

以上のアプローチを、グラフ描画問題の一種であるコンパクトメッシュ問題と地形図の簡約か問題に適用して実験を行った。特にコンパクトメッシュ問題においては、少数の頂点集合の縮約によってグラフの分枝幅をおさえることが可能であり、この方法の有効性を示唆する結果が得られている。実験対象としたデータの種類と個数が限られているため、より広範囲のデータに対して実験を計画している。

4 ハードウェア化の検討と技法の研究

大規模な組合せ問題を解く場合問題を専用のハードウェアで解かせる場合，そのハードウェアの構成は大きく分けて２つの形式が考えられる（並列コンピュータなどは除く）：

1. 組合せ問題を解く大規模な専用ハードウェア＋汎用コンピュータ
   汎用コンピュータは入出力などに使い，大規模計算には一切かかわらない

2. コプロセッサ（専用ハードウェア）＋汎用コンピュータ
   特定の時間がかかる部分のみを計算する専用ハードウェアで行わせる．この部分は実際はＰＣの拡張バスなどにカードとして挿す形態となる。

(１）の方法は，高性能が見込まれるが高価である．(２）の方法は，安価ではあるが，バスの通信スピードがボトルネックとなりスピードアップの高価が薄くなることが問題となる。

我々は，実際にシステムを構築することを考えているので費用の点で (２）の方式をとらざるをえない．そこで，大規模問題をコンパクトに格納すること，高速な演算を行うことを目標に LUT カスケードというメモリを直列多段に接続する論理関数の格納法・計算法を FPGA 上で実現し，一回の通信でなるべく多くの計算を専用ハードウェアで高速に計算させることを目標にこのアーキテクチャの有効性を検討した。専用ハードウェアとしては FPGA (Field Programmable Gate Array) を利用するのが現実的であるが，その開発ツールの習熟度および FPGA の特性の深い知識が，高性能化への必須条件である。そこで 2004 年は，FPGA を使用したシステムの試作を行うことを通じて，この FPGA 開発ツールの習熟や FPGA の特性を知ることを目標として研究をすすめた。

参考文献

[1] S. Arnborg and D.G. Corneil and A. Proskurowski, Complexity of finding embeddings in a k-tree, SIAM Journal on Algebraic and Discrete Methods, 8: 277-284, 1987

[2] S. Arnborg and J. Lagergren and D. Seese, Easy problems for tree-decomposable graphs, Journal of Algorithms, 12: 308-340, 1991

[3] H.L. Bodlaender, A Linear-Time Algorithm for Finding Tree-Decompositions of Small Treewidth, SIAM Journal on Computing, 25: 1305-1317, 1996.

[4] E.D. Demaine and M.T. Hajiaghayi and N. Nishimura and P. Ragde and D.M. Thilikos, Approximation algorithms for classes of graphs excluding single-crossing graphs as minors, Journal of Computer and System Sciences, 69-2: 166-195, 2004.

[5] N. Robertson and P.D. Seymour, Graph minors I. Excluding a forest, Journal of Combinatorial Theory, Series B, 35: 39-61, 1983

[6] N. Robertson and P.D. Seymour, Graph minors. II. Algorithmic aspects of tree-width, Journal of Algorithms, 7: 309-322, 1986

[7] N. Robertson and P.D. Seymour, Graph minors. X. Obstructions to tree-decomposition, Journal of Combinatorial Theory, Series B, 52: 153-190, 1991

[8] P.D. Seymour and R. Thomas, Call Routing and the Ratcatcher. Combinatorica, 14(2), 217-241, 1994

研究業績一覧

学術論文

1. Holger Bast, Kurt Mehlhorn, Guido Schäfer, Hisao Tamaki:
“Matching Algorithms Are Fast in Sparse Random Graphs”, Proc. of the 21st Symposium on Theoretical Aspects of Computer Science (STACS04), LNCS 2996, 81-92, 2004 年 3 月.
概要: c をある程度大きい正の定数とするとき、頂点数が n で辺の本数が cn のランダムグラフ（またはランダム 2 部グラフ）において、任意の非最大マッチングは長さ $O(\log n)$ の増加路を高確率で持つことを示した。このことは、代表的なマッチングアルゴリズムがそのようなランダムグラフ上で高速であることを意味する

2. Tetsuo Asano, Naoki Katoh, Hisao Tamaki, Takeshi Tokuyama:
“On Geometric Structure of Global Roundings for Graphs and Range Spaces”, Proc. of the 9th Scandinavian Workshop on Algorithm Theory (SWAT04), LNCS 3111, 455-467, 2004 年 10 月.
概要: ハイパーグラフ H と H の頂点をインデックスとする [0,1]-値のベクトルが与えられたとき、そのベクトルの大域丸めとは、2 進値ベクトルで、H のどの辺においても、もとのベクトルの要素の総和丸めベクトルの要素の総和の差が 1 未満であるようなものを言う。我々は両立集合の概念を用いて、大域丸めの集合のなす構造を調べる。ハイパーグラフが最短路公理と呼ばれる公理集合を満たすときには、大域丸めの個数が $n+1$ 個以下である（n はハイパーグラフの頂点数）と予想し、この予想がいくつかの幾何的レンジスペースや、直並列グラフの最短路ハイパーグラフに対しては成り立つことを示した。

3. Tetsuo Asano, Naoki Katoh, Hisao Tamaki, Takeshi Tokuyama:
“The structure and number of global roundings of a graph”, Theoretical Computer Science, 325-3, 425-437, 2004 年１０月.
概要: グラフの各頂点に実数値が割り当てられているときに、それらの値を整数値に丸めたい。このとき、あらかじめ定められた頂点集合族に属する集合のそれぞれにおいて、もとの値の合計と丸め結果の合計の差が 1 未満であるという大域的な条件をつける。頂点集合族として、グラフの最短路上の頂点集合をとった場合について、制約を満たす丸めの集合の構造を調べ、木、サイクルや、それらを拡張したグラフに対して、丸めの個数が常に $n+1$ 以下であることを示した。

4. Qiangping Gu, Hisao Tamaki:
“Optimal branch-decomposition of planar graphs in $O(n^3)$ time”, Simon Fraser University School of Computing Technical Report, SFU-CMPT-TR 2004-14, 1-12, 2004 年１１月.
概要: n 頂点の平面グラフ G が与えられたとき、G の分枝分割で幅が最小であるようなものを求める $O(n^3)$ 時間のアルゴリズムを与える。これはこれまでの最良の Seymour と Thomas による $O(n^4)$ 時間アルゴリズムを改良するものである。

5. Marin Dietzfelbinger, Hisao Tamaki:
“On the probability of rendezvous in graphs”, Random Structures and Algorithms, 26-3, 266 - 288, 2005 年 3 月.
概要: グラフにおいて、各頂点がその隣接点のひとつを当確率で選ぶという実験を考える。この実験において、お互いを選びあうような頂点対が生ずればランデブーが起きたという。この論文では、頂点数を一定にしたとき、ランデブー起きる確率が最も高いのは完全グラフであることを証明する。また、与えられたグラフに対してランデブーの起きる

確率を計算する問題は#P 完全であることを示す。

6. S. Nagayama, T. Sasao, Y. Iguchi, and M. Matsuura:
"Area-time complexities of multi-valued decision diagrams", IEICE Transactions on Fundamentals of Electronics, Vol.e87-A, No.5, pp.1020-1028, May 2004.
概要: This paper considers Quasi-Reduced ordered Multi-valued Decision Diagrams with k bits (QRMDD(k)s) to represent binary logic functions. Experimental results show relations between the values of k and the numbers of nodes, the memory sizes, the numbers of memory accesses, and area-time complexity for QRMDD(k). For many benchmark functions, the numbers of nodes and memory accesses for QRMDD(k)s are nearly equal to $1/k$ of the corresponding Quasi-Reduced ordered Binary Decision Diagrams (QRBDDs), and the memory sizes and the area-time complexities for QRMDD(k)s are minimum when $k = 2$ and $k = 3 - 6$, respectively.

7. H. Qin, T. Sasao, M. Matsuura, K. Nakamura S. Nagayama, and Y. Iguchi:
"A realization of multiple-output functions by a look-up table ring", IEICE Transactions on Fundamentals of Electronics, Vol.e87-A, 3141-3150, Dec. 2004.
概要: A look-up table (LUT) cascade is a new type of a programmable logic devices (PLDs), which provides an alternative way to realize multiple-output functions. Two types of LUT cascades exist: A combinational LUT cascade, and a sequential LUT cascade. Compared with a combinational LUT cascade, the sequential LUT cascade is more flexible. Unlike FPGA realization of a logic function, accurate prediction of the delay time is relatively easy in a sequential-LUT cascade realization. A prototype of a sequential LUT cascade has been custom-designed with 0.35

8. Y. Iguchi, T. Sasao, and M. Matsuura:
"A method to evaluate logic functions in the presence of unknown inputs using LUT cascades", Proc. of the 34th International Symposium on Multiple-Valued Logic (ISMVL-2004), 302-308, May 19-22, 2004.
概要: In logic simulation, we often need to evaluate two-valued logic functions in the presence of unknown inputs. However, a naive method often produces imprecise results. In these case, we can obtain precise values by evaluating the regular ternary logic function for the given two-valued logic function. This paper shows a hardware realization of regular ternary logic functions. We use look-up table (LUT) cascades to implement double-rail logic representation. The evaluation time for n-input logic function is O(n). They require much smaller amount of hardware than naive memory implementations.

9. T. Sasao, H. Nakahara, M. Matsuura, and Y. Iguchi:
"Realization of sequential circuits by look-up table ring", Proc. of The 2004 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS 2004), I-517-I-520, July 25-28, 2004.
概要: The LUT ring is a new type of memory-based realization of a sequential circuit that requires much smaller memory than conventional methods. In this paper, a method to realize a sequential circuit by a look-up table (LUT) ring is presented. The sequential circuit consists of a combinational part and feedback flip-flops. The combinational part is represented by a set of LUT cascades, and they are sequentially emulated by the LUT ring. The LUT ring uses two types of clocks: One evaluates the combinational part, and the other is the

clock for state transitions of the sequential circuit. We present a method to reduce the clock period for state transitions, given limited memory size.

研究会等

1. 井口幸洋, 鈴木隆広, 笹尾 勤:
"LUT リングを用いたプログラマブル・コントローラの構成法", 電子情報通信学会 第 2 種研究会 リコンフィギャラブルシステム研究会 (RECONF), pp.41-49, 2004 年 9 月 15 日.
概要: LUT(Look-Up Table) の出力の一部を入力にリング状に接続した LUT リングを用いてプログラマブル・ロジック・コントローラ (PLC: Programmable Logic Controller) を構成する方法を提案する．PLC で実行する命令の多くは，論理演算である. 同時に実行可能な論理演算をまとめ, 全ての組合せに対する出力値を予め計算して一つの LUT に蓄える．これらの LUT を個別に実装するかわりに, 一個のメモリを繰り返しアクセスすることにより複数の LUT として実現し, 出力の一部は外部出力レジスタに, 残りは状態変数レジスタに記憶し処理を進める．PLC のプログラミング入力としては，ラダー図を用いる．LUT 内部に格納するデータ, および, 出力を外部出力や内部記憶用に振り分けるための制御回路データを生成するツールも開発した．いくつかのベンチマーク関数に対する性能評価を示し, 従来の PLC よりも高速であることを示す.

2. 田中克征, 吉住謙一, 中村和之, 笹尾勤, 松浦宗寛, Qin Hui, 井口 幸洋:
"LUT カスケードアーキテクチャによるプログラム可能 LSI の開発,", 電子情報通信学会 第 2 種研究会・第 8 回システム LSI ワークショップ, pp.315-318, 2004 年 11 月 30 日.
概要: LUT カスケードアーキテクチャによるプログラム可能 LSI の開発を行い，チップ試作を行った. 動作速度，チップ面積，消費電力について FPGA との比較を行い, LUT カスケードアーキテクチャの有効性を示す

3. Hui QIN, 笹尾勤, 井口幸洋:
"A design of AES encryption circuit with 128-bit keys using look-up table ring", 電子情報通信学会 VLSI 設計技術研究会, VLD2004-122, 2005 年 01 月 26 日.
概要: This paper presents a partial-rolling architecture for an AES encryption processor. By using a look-up table ring and pipeline techniques, the proposed architecture reduces the amount of memory by 75% while maintaining the memory efficiency (i.e., throughput divided by the size of memory for core). We implemented two architectures: AES-4SM and AES-8SM on Altera Stratix FPGA. The AES-4SM achieved 5.61 G-bit/s throughput by using 20 memory blocks (M4Ks), and the AES-8SM achieved 10.49 G-bit/s throughput by using 40 M4Ks. We also implemented the unrolling architecture that achieves 20.48 G-bit/s throughput by using 80 M4Ks on the same FPGA. Compared with the unrolling implementation, the AES-4SM and the AES-8SM improved the memory efficiency by 10.9% and 18.2%, respectively, and reduced the amount of the memory blocks by 75% and 50%, respectively. The proposed implementation AES-8SM has an higher memory efficiency than both the fastest unrolling implementation and the fastest rolling implementation designed by other group. The proposed implementation fills gap between the rolling and unrolling implementations, and fits on less expensive FPGA.

4. 笹尾勤, 井口幸洋, 鈴木隆広:
"FIR フィルタの LUT カスケードによる実現について", 電子情報通信学会 VLSI 設計技術研究会, VLD2004-126, 2005 年 03 月 10 日.
概要: 本論文では，FIR フィルタのビット分散演算を表す関数として, n 入力 q 出力 DA 関数を定義する. 次に, DA 関数を k 入力 q 出力のセルを用いた LUT カスケードで実現する場合，単一の ROM で実現する場合に比べ

必要メモリ量を大幅に削減でき, セル数, メモリの総ビット数が量子化ビット数, タップ数, セルの入力数が決まれば上限が見積もれることを示す.

5. 井口幸洋, 笹尾勤:
“Walsh 係数を計算するハードウェアについて”, 電子情報通信学会 VLSI 設計技術研究会, VLD2004-127, 2005 年 03 月 10 日.
概要: 論理関数の Walsh スペクトラムの係数の一部をハードウェアを用いて計算する方法を示す. まず, Walsh 変換木を定義し, Walsh 変換木から Walsh 係数を計算する方法を示す. 次に, この操作をハードウェアで実現する方法を示す. 1 個の係数を計算するハードウェア量は, $O(2^n)$ であり, 全ての係数を求めるハードウェア量は, $O(n^2 \cdot 2^n)$ である. FPGA デバイス対して回路設計を行った結果, 市販 FPGA 上で計算可能な論理関数の変数の個数 14 であった. また, マイクロプロセッサに比べて FPGA 実現は, $n = 14$ のとき 1253 倍高速である.

A05: ハードウェアアルゴリズムの性能評価に関する研究

高木 直史　高木 一義

名古屋大学 大学院 情報科学研究科
〒 464-8603 名古屋市千種区不老町
{ntakagi,ktakagi}@is.nagoya-u.ac.jp

1　はじめに

集積回路技術の進展に伴い、これまでソフトウェアでは実現できなかった高度の実時間処理を、専用回路を構成して実現することが可能になってきている。すなわち、専用回路を構成することにより、処理時間に関わる計算限界を打破することが可能となってきている。このような専用回路を開発する場合、並列処理による高速計算や集積回路化に適した規則正しい回路構造等を意識した、ハードウェア実現向きのアルゴリズム、すなわち、「ハードウェアアルゴリズム」を設計することが重要である。

ハードウェアアルゴリズムの性能は、従来、アルゴリズムに基づく回路の、組合せ回路モデル上での段数や素子数、VLSI モデル上での面積等で評価してきた。しかし、集積回路技術の進展に伴い、これらのモデルおよび評価基準は、現実に即さなくなってきている。たとえば、回路の微細化に伴い、論理素子間を結ぶ配線における遅延が論理素子における遅延に対して無視できなくなってきており、回路の段数のみで計算時間を見積もることができなくなってきている。また、携帯機器等に用いられる回路の重要な性能要件である消費電力を見積もるための評価基準が定められていない。

本研究は、ハードウェアアルゴリズムの性能の、より現実に即した評価基準の確立を目的としている。具体的には、配線遅延や消費電力の評価を可能とする回路モデルを定め、配線遅延を考慮した計算時間の評価基準、および、消費電力の評価基準を確立することを目指している。

平成 16 年度は、既存のハードウェアアルゴリズムを従来の性能評価基準に従って体系的に分類し、「算術演算のＶＬＳＩアルゴリズム」と題する著書にまとめるとともに、これまでの研究で開発してきた回路設計資産の整理に着手した。また、現在の集積回路技術について調査し、ハードウェアアルゴリズムの新しい性能評価基準としてどのようなパラメータを定量化する必要があるかを検討した。具体的には、以下の研究を行った。

1. Karatsuba の方法に基づく乗算のハードウェアアルゴリズム

   集積回路技術の進展による配線層数の増加を考慮し、配線の容易さよりも素子数の少なさを優先した、乗算の新しいハードウェアアルゴリズムを開発し、スタンダードセル方式のＬＳＩ上に実現した場合の計算時間および面積を評価した。

2. 冗長２進表現の絶対値計算を用いた整数除算のハードウェアアルゴリズム

   組合せ回路モデル上での段数が演算数の長さに比例し、素子数が演算数の長さの平方に比例し、また、ＶＬＳＩモデル上での面積が演算数の長さの平方に比例する、新しい整数除算のハードウェアアルゴリズムを開発した。

3. 算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成システム

   ハードウェアアルゴリズムの性能の見積りを基に、アルゴリズム中のさまざまなパラメータを決定する、算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成システムを構想し、開発を開始した。

以下、これらの研究の詳細を述べる。

2 Karatsubaの方法に基づく乗算のハードウェアアルゴリズム

スタンダードセル方式のVLSIにおいては、配線層数の増加により配線の複雑化による面積の増加量が小さくなり、セルの総面積が回路面積に直接反映されるようになってきた。本研究では、多倍長乗算のソフトウェア実装においてしばしば用いられるKaratsubaの方法[1]に基づく、配線が複雑であるが素子数の少ない乗算器を設計し、小面積の並列乗算器が実現可能であることを示す。評価の結果、本研究の乗算器は配列型乗算器よりも高速かつ小面積であった。

2.1 Karatsubaの方法に基づく並列乗算器

Nビット符号なし2進整数の乗算について考える。被乗数Xと乗数Yを上位$k_H = \lceil N/2 \rceil$ビットと下位$k_L = \lfloor N/2 \rfloor$ビットにわけ、それぞれ$X_H, X_L, Y_H, Y_L$と表す（$X = 2^{k_L}X_H + X_L, Y = 2^{k_L}Y_H + Y_L$）。これらを用いて積$XY$を表すと、$XY = 2^{2k_L}X_HY_H + 2^{k_L}(X_HY_L + X_LY_H) + X_LY_L = 2^{2k_L}P_1 + 2^{k_L}(P_3 - P_1 - P_2) + P_2$となる。ここに$P_1 = X_HY_H$、$P_2 = X_LY_L$、$P_3 = (X_H + X_L)(Y_H + Y_L)$である。

Karatsubaの方法では、上式に従いP_1, P_2, P_3を計算する約$N/2$ビットの乗算3回と、加算、減算、シフトでNビットの乗算を行う。本研究ではアルゴリズムを再帰的に適用せず、一度だけ適用した乗算器を設計する。一般的な並列乗算器はおよそN^2個の全加算器が必要であるが、Karatsuba乗算器では$N/2$ビットの乗算3回におよそ$\frac{3}{4}N^2$個のFAですむため、素子数が少なくなる。

本研究で設計するKaratsuba乗算器は、P_1, P_2, P_3の計算に配列型乗算器やWallace木による乗算器を用いる。ここでP_3を求める際に桁上げ伝搬加算器を使用せず、P_3の部分積とP_1, P_2をともに足しあわせる。乗算器の中で利用する桁上げ伝搬加算器として、順次桁上げ加算器や桁上げ先見加算器を用いる。これらの乗算器や加算器の組み合わせによって、さまざまな特徴をもつ乗算器が構成できる。

2.2 Karatsuba乗算器の高速化

本研究では、次の二つの高速化手法を導入する。

一つは、P_1とP_2の各ビットと、P_3の部分積の各ビットの生成時間を考慮し、早く求まるビットから順に、全加算器や半加算器で足し合わせていくものである。全体の遅延がバランスされ、計算が高速化される。計算に必要な全加算器や半加算器の数は変らないので、素子数はほとんど増加しない。

もう一つは、P_1, P_2を求める乗算器において、最終段の桁上げ伝搬加算器を除去し、P_1, P_2を桁上げ保存形で出力するものである。これにより乗算器内での桁上げ伝搬がなくなり、高速化できる。ただし、P_1, P_2は、二カ所で用いるので、後段の加算および減算のためのハードウェア量が増加する。

2.3 乗算器の評価

上述の方法を組み合わせたさまざまな32ビット符号なし整数Karatsuba乗算器を、Verilog HDLにより設計し、ライブラリとしてVDEC ROHM0.35μmを用いて論理合成を行った。また配列型乗算器やWallace木による乗算器を同様の条件で設計し、遅延、面積の比較を行った。結果を図2.1に示す。Wallace木の乗算器と比較すると遅延で劣るものの、配列型乗算器に対しては高速かつ小面積となっていることが確認できる。最も小さな面積の配列型乗算器と比較して、85%にまで小型化することができた。

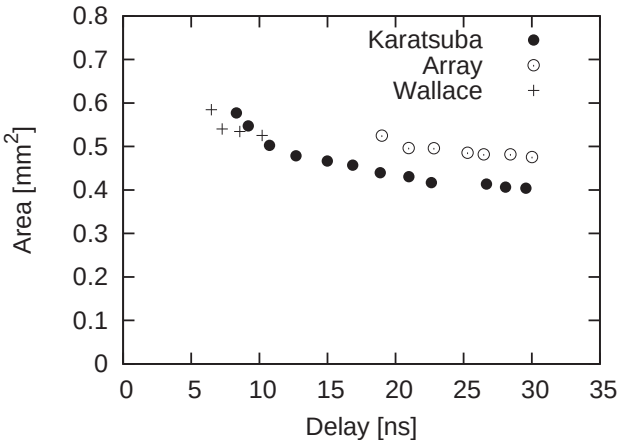


図2.1: 32ビット符号なし整数乗算器の遅延と面積

3 冗長２進表現の絶対値計算を用いた整数除算のハードウェアアルゴリズム

整数除算は、基本算術演算の一つであり、いくつかの整数除算器が市販のＩＰライブラリに登録されている [2]。整数除算は、プロセッサにおいて多くのクロックサイクルを要する演算であり、サイクル数は演算数の値によって可変となる。

本研究では、整数除算のハードウェアアルゴリズムを提案する。アルゴリズムは減算シフト型の非回復型除算法に基づいている。専用回路によって計算を高速化するには、部分剰余の表現に桁上げ保存形や符号付きディジット表現 [3] を導入し、漸化式の計算を桁上げの伝搬なしに高速に行う手法がよく用いられる [4]。しかし、そのためには、除数を正規化する必要があり、したがって、大きな面積を要する先頭１検出器やバレルシフタが必要となる。

本研究で提案するハードウェアアルゴリズムでは、部分剰余を基数２の符号付きディジット表現（２進ＳＤ表現）で表し、漸化式の計算を桁上げの伝搬なしに高速に行い、かつ、除数の正規化を必要としない。部分剰余を符号と絶対値の組で保持し、絶対値を２進ＳＤ表現で表す。商の各桁は部分剰余の符号から決定する。漸化式の計算において、符号の計算と絶対値の計算を並行に行う。絶対値の計算は、前の部分剰余の符号が未知でも開始できる。

アルゴリズムに基づく除算器の組合せ回路モデル上での段数は演算数の長さに比例し、素子数は演算数の長さの平方に比例する。また、ＶＬＳＩモデル上での面積は演算数の長さの平方に比例する。

3.1 非回復型整数除算

ここでは、n ビット２の補数表示２進整数である被除数 X と除数 Y $(\neq 0)$ から、$X = Y \times Z + R$ を満す、n ビット２の補数表示２進整数の商 Z と剰余 R を求めるものとする。ただし、R は X と同じ符号になるようにする。

提案アルゴリズムは、以下に示す基数２の非回復型整数除算アルゴリズムに基づく。

[Algorithm IDIV]
$D := |Y|$; $R_n := X$;
for $j := n-1$ downto 0 do
  if $R_{j+1} = 0$ then do
    $Q := [q_{n-1}q_{n-2}\cdots q_{j+1}0\cdots 0]$; $R := 0$;
    go to label;
  endif;
  if $R_{j+1} < 0$ then $q_j := -1$ else $q_j := 1$ endif;
  $R_j := R_{j+1} - q_j \cdot 2^j \cdot D$;
endfor;
$Q := [q_{n-1}q_{n-2}\cdots q_0]$;
if $X > 0$ and $R_0 < 0$
  then $R := R_0 + D$; $Q := Q - 1$;
 elseif $X < 0$ and $R_0 > 0$
  then $R := R_0 - D$; $Q := Q + 1$;
 else $R := R_0$;
endif;
label: if $Y < 0$ then $Z := -Q$ else $Z := Q$ endif;
□

Q は、$R_{j+1} = 0$ となるまで、-1 と $+1$ の系列として求まる。Q の２の補数表示２進表現 $P = [p_{n-1}p_{n-2}\cdots p_0]$ $(p_j \in \{0,1\})$ は、$R_{j+1} = 0$ となる j を j_0 とする（そのような j がない場合は $j_0 = -1$ とする）と、$j_0 + 2$ 以上の j については q_{j-1} が -1 なら p_j を 0、$+1$ なら 1 とし、p_{j_0+1} を 1 とし、j_0 以下の j については p_j を 0 とすることにより求まる。

3.2 ２進ＳＤ整数の符号と絶対値の計算

２進ＳＤ表現は桁集合が $\{-1, 0, 1\}$ の２進表現である。提案する除算アルゴリズムでは、２進ＳＤ整数の符号と絶対値の計算が必要である。２進ＳＤ整数の符号は、その中の最上位の非零桁の符号である。また、絶対値（の２進ＳＤ表現）は、その数が負である場合、各桁の符号を反転することにより求まる。

以下に、２進ＳＤ整数 $A = [a_{n-1}a_{n-2}\cdots a_0]$ の符号と絶対値を計算するアルゴリズム [5] を示す。得られる $sgn(A)$ は、A が正なら 1、零なら 0、負なら -1 である。$abs(A)$ は非負の２進ＳＤ整数である。

[Procedure SGNABS]

$s_n := 0$;
for $i := n-1$ downto 0 do
  if $s_{i+1} = 0$ and $a_i = -1$ then $s_i := -1$;
  elseif $s_{i+1} = 0$ and $a_i = 1$ then $s_i := 1$;
  else $s_i := s_{i+1}$;
  endif;
  if $s_i = -1$ and $a_i \neq 0$ then $b_i := -a_i$;
  else $b_i := a_i$ endif;
endfor;
$sgn(A) := s_0$;
$abs(A) := [b_{n-1}b_{n-2}\cdots b_0]$; □

3.3 整数除算のハードウェアアルゴリズム

提案アルゴリズムは、[Algorithm IDIV] に基づく。構造の規則性を増すために、途中で $R_{j+1} = 0$ となっても $q_j = 1$ として計算を続ける。[5] と同様に、数列 $\hat{R}_j = sign(R_{j+1}) \cdot R_j$ を導入し、2進SD表現で表す。定義より、$|\hat{R}_j| = |R_j|$、
$sign(\hat{R}_j) = sign(R_{j+1}) \cdot sign(R_j)$ $(R_j \neq 0)$、
$sign(\hat{R}_j) = +1$ $(R_j = 0)$
が成り立つ。よって、元の R_j の符号は、
$sign(R_j) = sign(R_{j+1}) \cdot sign(\hat{R}_j)$ $(R_j \neq 0)$、
$sign(R_j) = +1$ $(R_j = 0)$
となる。$sign(R_{j+1}) = -1$ のとき $R_j = R_{j+1} + 2^j \cdot D$ 他のとき $R_j = R_{j+1} - 2^j \cdot D$ であるから、$\hat{R}_j = |\hat{R}_{j+1}| - 2^j \cdot D$ である。$|\hat{R}_{j+1}|$ は、$\hat{R}_{j+1}$ から、[Procedure SGNABS] により求まる。したがって、$\hat{R}_j$ は $sign(R_{j+1})$ と独立に計算できる。すなわち、$\hat{R}_j$ と $|\hat{R}_j|$ の計算を $R_{j+1}(\hat{R}_{j+1})$ の符号がわかる前に開始できる。

右にハードウェアアルゴリズムを示す。D は Y が正なら Y、負なら $\bar{Y}+1$ である。ここに、$\bar{Y}$ は Y のビット毎の反転である。補正の +1 ビットは $\hat{R}_j$ の計算における最下位への桁借り入力として扱う。P の -1 補正は、最下位ビットを 1 から 0 にすることにより容易に行える。一方、+1 補正は、$p_j = 0$ である最小の j を j_1 とすると、j_1 以下の j について p_j をビット反転することにより行える。2進表現の剰余 R を得るために、2進SD／2進変換が必要である。

[Hardware Algorithm IDIV-HA]

if $y_{n-1} = 0$ then $D := Y$ else $D := \bar{Y} + 1$ endif;
$\hat{R}_n := X$;
if $x_{n-1} = 1$ then $sign(R_n) := -1$
 else $sign(R_n) := +1$ endif;
for $j := n-1$ downto 0 do
 if $sign(R_{j+1}) = -1$ then do
  if $y_{n-1} = 0$ then $p_{j+1} := 0$
   else $p_{j+1} := 1$ endif;
 else do
  if $y_{n-1} = 0$ then $p_{j+1} := 1$
   else $p_{j+1} := 0$ endif;
 endif;
 $\hat{R}_j := |\hat{R}_{j+1}| - 2^j \cdot D$;
 $|\hat{R}_j| := abs(\hat{R}_j)$;
 if $sgn(\hat{R}'_j) = -1$
  or ($sgn(\hat{R}'_j) = 0$ and $sign(R_{j+1}) = -1$) then
   $sign(R_j) := -sign(R_{j+1})$
 else $sign(R_j) := sign(R_{j+1})$ endif;
endfor;
$P := [p_{n-1}p_{n-2}\cdots p_1 1]$;
if $x_{n-1} = 0$ then do
  if $sign(R_0) = -1$ then do
   $R := |\hat{R}^*_0|$;
   if $y_{n-1} = 0$ then $Z := P - 1$
    else $Z := P + 1$ endif;
  else $R := |\hat{R}_0|$; $Z := P$;
  endif;
else do
  if $sgn(\hat{R}^*_0) = 0$ then do
   $R := -|\hat{R}^*_0|$;
   if $y_{n-1} = 0$ then $Z := P - 1$
    else $Z := P + 1$ endif;
  elseif $sgn(\hat{R}_0) \neq 0$ and $sign(R_0) = +1$
   then do
   $R := -|\hat{R}^*_0|$;
   if $y_{n-1} = 0$ then $Z := P + 1$
    else $Z := P - 1$ endif;
  else $R := -|\hat{R}_0|$; $Z := P$;
  endif;
endif; □

4 算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成

プロセッサ等の開発において、種々の信号処理やコンピュータグラフィックス等のために、より高い演算性能を実現するためには、処理に頻出し、時間のかかる算術演算のための専用回路を開発することが有効であると考えられる。このような演算の例として、平方根の逆数計算や立方根計算等が挙げられる。

本研究では、算術演算のための減算シフト型ハードウェアアルゴリズム [4] の自動合成について考察する。自動合成においては、まず、与えられた演算に対し、これを加減算とシフト、一桁の乗算の繰返しで計算する漸化式を生成し、さらに、計算に用いる基数や桁集合等から桁選択関数を定め、具体的なアルゴリズムを設計する必要がある。この際、ハードウェアアルゴリズムの性能の見積りを基に、アルゴリズム中のさまざまなパラメータを決定する。

以下では、まず、与えられた演算の算術式から、減算シフト型アルゴリズムのための漸化式を生成する方法の概要を示し、次に、漸化式および基数、桁集合等から桁選択関数を求める手順の概要を述べる。

4.1 漸化式の生成

計算したい演算が算術式 f で与えられたときに、これに対する減算シフト型アルゴリズムのための漸化式を生成する手順について考える。f は、オペランドおよび加算、減算、乗算、除算（逆数計算も含む）、m 乗根（m は正の整数）の組合せで表されるとする。オペランドの個数は任意とする。f に対し、計算が加減算、シフト、一桁の乗算のみで行えるような漸化式を生成する。手順は以下の通りである。

まず、f に対し、残余 $W[j]$ の式を求める。f の算術式の各項について、$\frac{A}{B}$ があれば、式を $\frac{A}{B} = M$ として両辺に B を掛け、$A(B)^{\frac{1}{m}}$ があれば、式を $A(B)^{\frac{1}{m}} = M$ として両辺を m 乗じ、式を展開する。この操作を、式の各項に除算、m 乗根が存在しなくなるまで繰り返し、最後に、式を $g = 0$ の形に変形する。g には除算や m 乗根が存在しない。得られた $g = 0$ から、残余 $W[j]$ の式を、g を r^j 倍することにより得る。すなわち、

$$W[j] = r^j g \tag{2.1}$$

である。

次に、残余の漸化式を求める。漸化式は、式 (2.1) の j を $j+1$ に置き換え、中間結果の漸化式

$$S[j+1] = S[j] + s_{j+1} r^{-j-1} \tag{2.2}$$

を代入して展開することにより得られる。

$$W[j+1] = rW[j] + \cdots \tag{2.3}$$

の式で表される。ここで、得られた $W[j+1]$ の漸化式中に、オペランドと中間結果との乗算が存在するかを調べる。存在した場合、新しい中間変数で置き換える。さらに、新たに導入した変数に対する漸化式を導出する。乗算が漸化式中に存在しなくなるまでこの処理を繰り返す。

4.2 桁選択関数の生成

漸化式と基数 r、桁集合 $\{-a, \cdots, -1, 0, 1, \cdots, a\}$ 等から桁選択関数を生成する手順について考える。$\frac{r}{2} \leq a \leq r-1$ とする。手順は以下の通りである。

まず、与えられた漸化式と基数、桁集合から、s_{j+1} として k を選んでもよい $rW[j]$ の範囲 $L_k[j] \leq rW[j] \leq U_k[j]$ を求める。ここで、残余 $W[j]$ の満たすべき範囲を $\underline{B}[j] \leq W[j] \leq \overline{B}[j]$ とする。$W[j+1]$ が $\underline{B}[j+1] \leq W[j+1] \leq \overline{B}[j+1]$ を満たすように s_{j+1} を $\{-a, \cdots, -1, 0, 1, \cdots, a\}$ の中から選ぶ必要がある。$s_{j+1} = k$ としたときの残余の漸化式を $W[j+1] = rW[j] + H_k[j]$ と表すと、

$$L_k[j] = \underline{B}[j+1] - H_k[j] \tag{2.4}$$
$$U_k[j] = \overline{B}[j+1] - H_k[j] \tag{2.5}$$

となる。$k = -a$ に対する下限及び $k = a$ に対する上限がそれぞれ $rW[j]$ の下限及び上限となるので、

$$r\underline{B}[j] = \underline{B}[j+1] - H_{-a}[j] \tag{2.6}$$
$$r\overline{B}[j] = \overline{B}[j+1] - H_a[j] \tag{2.7}$$

を得る。これらの漸化式から $\underline{B}[j]$、$\overline{B}[j]$ を求め、式 (2.4)、(2.5) より $L_k[j]$、$U_k[j]$ を定める。

次に、得られた $L_k[j]$ 及び $U_k[j]$ から、桁選択関数を決定する。桁選択関数は、$rW[j]$ と、$L_k[j]$ および $U_k[j]$ に含まれる変数に依存する。しかし、r^{-j} が含まれる項は、j が増えると急速に小さくなるので、桁選択関数を、あるとしてもごく少数の小さな j についてを除き、その項の中に存在する変数に依存しないようにすることができる。

桁選択関数への各入力の見積り値から s_{j+1} の値を決定する。桁選択関数を、選択の境界となる値の集合 $\{m_k|k \in \{-a+1, \cdots, -1, 0, 1, \cdots, a\}\}$ で表す。$m_k \leq \widehat{rW}[j] < m_{k+1}$ ならば、s_{j+1} として k が選択される。ここに、$\widehat{rW}[j]$ は $rW[j]$ の見積り値である。また、m_k は $rW[j]$ 以外の桁選択関数への入力に依存する。m_k は、s_{j+1} として $k-1$ が選ばれる $rW[j]$ の範囲と k が選ばれる範囲の重なりの範囲から、桁選択関数への入力となる変数の表現方法や範囲等を考慮して定めればよい。

桁選択関数の実現方法としては、比較器による実現、テーブルによる実現が考えられる。テーブルによる実現ではさらに、テーブルを ROM で作るのか論理回路で作るのかの選択がある。ここでは、桁選択関数を比較器で実現する場合に適した生成について述べてきたが、テーブルで実現する場合には、エントリに自由度が存在する。そのため、どのエントリを選ぶべきかという問題がある。また、桁選択関数の入力に必要なビット数のパラメータ（本研究では t と d）にも自由度があり、いくつかの可能な組合せの中からどれを選択すればよいかという問題がある。選択の基準としては、入力ビット数の和、有効なエントリ数、積項数等がある。また、桁選択関数の実現方法により、最適な基数や桁集合の選び方も異ってくると考えられる。

以上のことから、よりよい回路を実現するためには、桁選択関数の生成では、ある程度の自由度がある状態で出力し、次の段階で、回路実現方法を考慮して最適な桁選択関数を選ぶ、という二段階に分けて考えることが必要である。

5 まとめ

Karatsuba の方法に基づく乗算のハードウェアアルゴリズムの研究により、配線層数の多いスタンダードセル方式の集積回路では、ＶＬＳＩモデル上での面積よりも、組合せ回路モデル上での素子数の方が、面積のより現実に即した評価基準になり得るという知見を得た。冗長２進表現の絶対値計算を用いた整数除算のハードウェアアルゴリズムの研究では、組合せ回路モデルおよびＶＬＳＩモデル上で性能評価基準において、従来よりも優れたハードウェアアルゴリズムを開発した。また、算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成システムを構想し、開発を開始したが、このシステムでは、ハードウェアアルゴリズムの性能の見積りが重要である。今後も、ハードウェアアルゴリズムの性能の、より現実に即した評価基準の確立を目指して、これらの研究を進める予定である。

参考文献

[1] A. Karatsuba and Yu. Ofman: ‘Multiplication of multidigit numbers on automata,’ Sov. Phys. Dokl., 7, pp.595-596, 1963.

[2] Synopsys Inc.: ‘DesignWare Building Block IP,’ 2003.

[3] A. Avizienis: ‘Signed-Digit number representations for fast parallel arithmetic,’ IRE Trans. Elec. Comput., vol. EC-10, no. 3, pp. 389-400, Sept. 1961.

[4] M. D. Ercegovac and T. Lang: “Division and Square Root – Digit-Recurrence Algorithms and Implementations,” Kluwer Academic Publishers, 1994.

[5] H. Dawid and H. Meyr: ‘The differential CORDIC algorithm: constant scale factor redundant implementation without correcting iterations,’ IEEE Trans. Comput., vol. 45, no. 3, March 1996.

研究業績一覧

著書

1. 高木直史:
   “算術演算のＶＬＳＩアルゴリズム（並列処理シリーズ５）”, コロナ社, 2005 年３月.
   概要: さまざまな信号処理や画像処理、画像圧縮／伸長、グラフィクス、暗号処理などのための専用回路がＶＬＳＩ上に実現されるようになり、「ＶＬＳＩアルゴリズム」の設計が重要になってきている。「ＶＬＳＩアルゴリズム」は、ＶＬＳＩ上での実現を前提として、並列処理や規則正しい回路構造を意識して設計されたアルゴリズムである。本書では、さまざまな専用回路において中心的な役割を果たす算術演算を主な対象として、種々のＶＬＳＩアルゴリズムを示し、その中で用いられている手法を紹介する。これらの手法は、さまざまな専用回路のためのＶＬＳＩアルゴリズムの設計に適用できる。また、算術演算の種々のＶＬＳＩアルゴリズムを理解することは、専用回路のためのＶＬＳＩアルゴリズムの設計において、最適な算術演算回路を選択するために必須である。

学術論文

1. M. .E. Kaihara, N. Takagi:
   “A Hardware Algorithm for Modular Multiplication/Division”, IEEE Transactions on Computers, Vol. 54, No. 1, pp. 12–21, January, 2005.
   概要: A mixed radix-4/2 algorithm for modular multiplication/division suitable for VLSI implementation is proposed. The algorithm is based on Montgomery modular multiplication and on the extended Binary GCD algorithm for modular division. Both algorithms are modified and combined into the proposed algorithm so that almost all the hardware components are shared. The new algorithm carries out both calculations using simple operations such as shifts, additions, and subtractions. The radix-2 signed-digit representation is used to avoid carry propagation in all additions and subtractions. A modular multiplier/divider based on the algorithm performs an n-bit modular multiplication/division in $O(n)$ clock cycles where the length of the clock cycle is constant and independent of n. The modular multiplier/divider has a linear array structure with a bit-slice feature and can be implemented with much smaller hardware than that necessary to implement both multiplier and divider separately

研究会等

1. カイハラ マルセロ，高木直史:
   “拡張ユークリッド法に基づく剰余系乗除算回路”, 電子情報通信学会技術研究報告, VLD2004-1, 1–6, 2004 年５月.
   概要: ＶＬＳＩ実現向きの剰余系乗除算回路を提案する。除算は拡張ユークリッド法、乗算は通常の乗算アルゴリズムとモンゴメリ乗算に基づく。通常の乗算は二倍の操作と加減算の繰り返しで行う。モンゴメリ乗算は新しく提案した左シフト型の手法に基づく。これらの演算はビットシフトや加減算などの単純な操作の繰り返しで行う。基数 2 の符号付きディジット表現を用いることにより全ての加減算を桁上げ伝播なしに行う。提案する剰余系乗除算回路は、規則正しいビットスライス構造を持ち、n ビットの剰余系乗算、モンゴメリ乗算及び剰余系除算を $O(n)$ クロックサイクルで実行する。クロックサイクルの長さは n に依存しない。提案する剰余系乗除算回路は、モンゴメリ法に基づく乗算回路、通常の剰余系乗算回路と剰余系除算回路を別々に設計したものより少ないハードウェア量で実装できる。

2. 小林克希，高木直史，高木一義:
   “GF(2^m) 上の逆元算出のための拡張ユークリッド法に基づくテーブルを用いたアルゴリズム”, 電子情報通信学会技術研究報告, VLD2004-2, 7–12, 2004 年５月.
   概要: $\mathbf{GF}(2^m)$ 上の逆元算出のための拡張

ユークリッド法に基づくテーブルを用いたアルゴリズムを提案する。提案アルゴリズムでは、従来の拡張ユークリッド法に基づく逆元算出アルゴリズムの数回の反復における演算を行列で表現し、事前に計算してテーブルに保持しておく。これにより、提案アルゴリズムをハードウェア実装した際に、従来よりもXOR の段数を削減することが可能となる。また、$w \times (w+1)$ ビットの $\mathbf{GF}(2^m)$ 上の乗算器を用いれば、ソフトウェア実装した際に多倍長演算の処理時間を削減し、高速化することが可能である。

3. 門脇俊介，高木直史，高木一義:
“冗長 2 進数の絶対値計算を用いた整数除算回路”，電子情報通信学会技術研究報告, VLD2004-3, 13–18, 2004 年 5 月.
概要: 非回復型の除算アルゴリズムに基づいた新しい整数除算回路を提案する。各部分剰余を冗長 2 進数で表し、その絶対値を計算するとともに、その部分剰余の符号も求めていくものである。その符号を用いて商の各桁を最上行桁から順に決定していく。n ビットの被除数、除数から n ビットの商と剰余を $O(n)$ の時間で計算できる。32 ビットの被除数、除数から 32 ビットの商と剰余を出力する整数除算器として、提案するアルゴリズムに基づく回路を組合せ回路として実現した。順次桁上げ加算器を用いて実現した非回復型整数除算器と比較すると、遅延時間は約 65%の減少であった。また、桁上げ先見加算器を用いて実現した非回復型整数除算器と比較すると、遅延時間は約 25%の減少であった。

4. 熊澤文雄，高木直史:
“算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成”, 電子情報通信学会技術研究報告, VLD2004-90，ICD2004-176，DC2004-76, 175–178, 2004 年 12 月.
概要: プロセッサ等の開発において、より高い演算性能を実現するためには、頻出する算術演算のための専用回路を開発することが有効であると考えられる。本報告では、算術演算の専用回路のための減算シフト型ハードウェアアルゴリズムの自動合成について考察する。計算したい演算が算術式として与えられたとき、加減算、シフト、一桁の乗算の繰り返しで計算が行えるような漸化式を生成する。漸化式、基数、桁集合、残余の表現方法などが与えられたとき、桁選択関数を生成する。

学会大会等

1. 高木直史，高木一義:
“冗長ＳＤ／非冗長２進のオンザフライ変換の新手法”, 情報処理学会第 67 回全国大会, 1, 13–14(6B-1), 2005 年 3 月.

2. 柴岡雅之，高木直史，高木一義:
“Karatsuba アルゴリズムに基づく小面積並列乗算器”, 2005 年電子情報通信学会総合大会, 基礎・境界, 66(A-3-1), 2005 年 3 月.

3. 小林克希，高木直史，高木一義:
“反復回数を削減した拡張ユークリッド法に基づく GF(2^m) 上の逆元算出アルゴリズム”, 2005 年電子情報通信学会総合大会, 基礎・境界, 67(A-3-2), 2005 年 3 月.

4. 高木直史:
“テーブルサイズを削減した逆数の区分二次近似法”, 2005 年電子情報通信学会総合大会, 基礎・境界, 68(A-3-3), 2005 年 3 月.

A06: 幾何的配置問題の計算量限界と近似可能性の研究

加藤 直樹　大崎 純　瀧澤 重志

京都大学 大学院 工学研究科
〒 615-8540 京都市西京区京都大学桂 C クラスター
{naoki,ohsaki,kukure}@archi.kyoto-u.ac.jp

1　はじめに

建築におけるトラス構造物の最適設計問題や、都市工学における通路、道路、鉄道などの配置問題および道路網などにおける配送問題は、数理的にはユークリッド幾何構造の上での最適化問題として特徴付けられる。また、これらの問題の多くは、実現可能な解集合を考慮すると本質的に離散構造を有する。たとえば、建築構造物の設計では、実現できる部材長や部材断面積は、あらかじめ与えられたサイズ集合から選択されるのが望ましい。通路、道路の配置問題、配送問題でも実現可能な幾何学的単位は限定される。本研究では、これらの問題を幾何的配置問題としてモデル化し、個々の問題の計算量限界を明らかにするとともに、離散組合せ手法や計算幾何学を用いて実用的に解ける近似アルゴリズムの開発することにより近似可能性について解析をおこなう。今年度において得られた主要な成果の概略は以下の通りである。

1. 存在することのできる節点と部材の位置が与えられたトラスに対し，静的外力の下での応力と，局所的な安定性の制約の下で最適な部材トポロジーを求める問題を，混合整数計画法として定式化し，分枝限定法で大域最適解を求めた (図 1)。また，選択可能断面リストの与えられた骨組の最適断面積を求める問題を，種々のヒューリスティックスを用いて解き，性能を比較した。(学術論文 2.)

2. 異なる部材長の数を最小にするトラスの設計問題を、異なる辺長の数を最小化する二次元平面上の三角形メッシュ生成問題としてモデル化し、計算量限界、近似性能比を明らかにした (図 2)。また、異なる節点のタイプの数を最小化するトラスの設計問題を、隣り合う辺間の角度の種類数を最小にする問題としてモデル化し、計算量限界、近似性能比を明らかにした。(研究会等 3.)

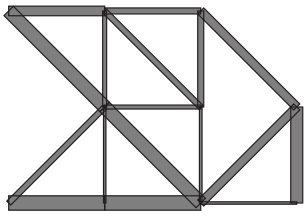


図 2.1: 最適トポロジー

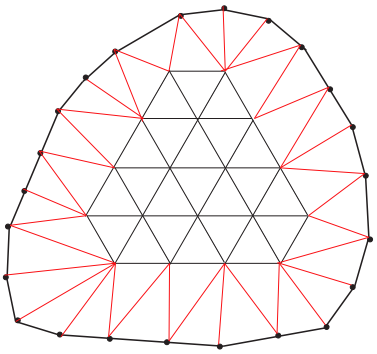
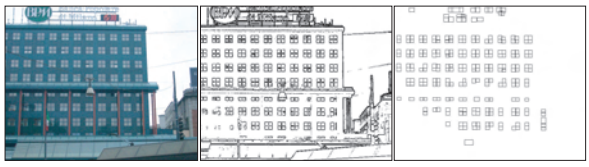


図 2.2: 三角形メッシュ

3. 平面上に存在する利用者間の交通量が与えられている時、総和が一定の長さの線分集合で表現される道路（または鉄道）を配置することにより増大する利用者の利便性を最大化する交通網を設計する問題を幾何的最適化問題としてモデル化し、計算量限界、近似性能比を明らかにする。(学会大会等 6.)

4. 2 値化エッジ画像からの高速長方形成分検出手法の開発: カラー画像やグレースケール画像に対して、2 値化処理が予め施された 2 値



原画像 640×480px　　二値化エッジ画像　　検出結果

図 2.3: 実験例

化エッジ画像を入力画像とし、1 枚の画像から実用的な計算時間で長方形集合を検出する方法を提案した。入力として画像に対して主軸方向が同一で、スライシング構造を持つ複数の長方形とする。本論文では、実用的な計算時間で高精度の長方形検出をおこなうため、次のようなさまざまな工夫をおこなっている (図 3)。(1) 長方形群の主軸 2 方向に沿ったスライス処理を施すことによって、長方形が存在する可能性の高い領域を限定する処理をおこなっている。そこで得られた領域ごとに、長方形検出のためのしきい値を適応的に設定することによって、欠損率の異なる長方形を一度に検出できるようにしている。(2) ノイズカットや濃度値データの計算といった前処理を施すことによって、計算効率と検出精度の向上を図っている。(3) 線形時間の動的計画法を利用して長方形の辺候補が存在する部分を絞り込むことによって、辺候補 4 本の組合せで得られる長方形候補の数を劇的に減らし、結果として計算時間の大幅な短縮を達成している。(学術論文 3.)

5. 配送問題では、積込み、配送の 2 種類の荷物を有する場合について、とくに取り扱うネットワークが木構造を有する場合について新しい近似アルゴリズムを開発した。車両の起点、終点は単一のデポに限定されている場合を扱う。効率のよい 2– 近似アルゴリズムを提案した。(学術論文 9.)

6. 与えられた平面上の点集合に対して、それらを k 個の折れ点のある区分線形関数で近似する問題（誤差評価は L_1 および L_2-距離）を取り扱い、近似解法を提案した (図 4)。(研究会等 4.)

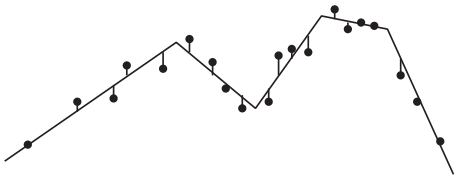


図 2.4: 点集合の折れ線近似

7. 区分線形非負実数値関数 $f : R^d \to R$ を単峰関数で近似するアルゴリズムを提案した。アルゴリズムは、最大流問題などのグラフアルゴリズムに基づくもので、得られた結果はデータマイニングにおける高次元領域ルールの生成に利用される。(研究会等 2.)

8. 平面上に与えられた長方形集合を結ぶ橋のなかで迂回率を最小にするものを求める問題を取り扱った。ある条件の下ではその問題が多項式時間で得られることを示した。(学術論文 6.)

9. リンク機構、テンセグリティの実現可能性、最適な組み立て順序, 最適張力に関する力学、幾何学を統合したモデル化をおこない、問題の計算量限界を明らかにした。(研究会等 6.)

なお、上記の項目 6,7,8 については A02 班や C05 班の班員との共同研究の成果である。

研究業績一覧

学術論文

1. 宮高泰昌，加藤直樹，瀧澤重志:
“建築画像データベースの自動索引付けを目指した建築構成要素の認識手法の開発 畳と格子を例として”, 日本建築学会環境系論文集, 第 588 号, pp.63-70, 2005.2.
概要: 建築画像データベースを構築することを最終目標として，建築画像の自動索引付けには，どのような検索キーを付与することが有用であるか，という点を考慮することが重要である。本研究では，建築画像データベースにおける有効な検索システムの構築を目指し，画像への自動索引付けを目的として,「画

像中に特定の建築構成要素を含むかどうか」を判別する方法を「畳」と「格子」を例として，二つ提案する。
提案する一つ目の方法は，特定の建築構成要素を含む画像は，画像内の大まかな色分布と構図も概ね似通っているという考え方を基礎に，パターン認識と類似画像検索の技術を応用することによって，画像内の色分布と構図情報の類似度を計算して判別を行おうとするものである。類似画像検索の研究において画像間の類似度として，建築画像を探す際に重要な観点や要素である,「色」と「構図」を考慮した研究も存在する。しかし，それらの研究では構図情報の抽出に複雑な領域分割処理を行うものが多く，処理に手間がかかる上，必ずしも建築的な構図を反映したものではなかった。そこで本研究では，画像内の画素の位置情報が建築画像の構図にとって重要であると考え，粗く切った画像において「色と構図の情報」を考慮した類似度を，最小費用流問題によって計算する方法を提案する。
二つ目は，画像認識技術を用いて特定の構成要素に対して，その判別に重要な役割を果たす特徴量を抽出することにより，構成要素の存在の有無に関する学習モデルを構築し，判別を行う方法である。
判別精度は 7,8 割とまだ実用レベルには達していないが，既に実用化されている文字認識などと比較した場合に，建築構成要素のもつ構図や対象の多様性を考慮すると，研究初期段階の目的は達したものと考えられる。

2. M. Ohsaki and N. Katoh:
“Topology optimization of trusses with stress and local consraints”, Structural and Multidisciplinary Optimization, 29, 190-197, 2005.3.
概要: A truss topology optimization problem under stress constraints is formulated as a Mixed Integer Programming (MIP) problem with variables indicating existence of nodes and members. The local constraints on nodal stability and intersection of members are considered, and a moderately large lower bound is given for the cross-sectional area of an existing member. A lower-bound objective value is found by neglecting the compatibility conditions, where linear programming problems are successively solved based on a branch-and-bound method. An upper-bound solution is obtained as a solution of NonLinear Programming (NLP) problem for the topology satisfying the local constraints. It is shown in the examples that upper- and lower-bound solutions with small gap in the objective value can be found by the branch-and-bound method, and the computational cost can be reduced by using the local constraints for obtaining a practically optimal solution.

3. 天沼はるか、加藤直樹:
“2 値化エッジ画像からの高速長方形成分検出手法の開発”, 日本建築学会環境系論文集, No.586, 83-90, 2004 年 12 月.
概要: 本研究では、カラー画像やグレースケール画像に対して、2 値化処理が予め施された 2 値化エッジ画像を入力画像とし、1 枚の画像から実用的な計算時間で長方形集合を検出する方法を提案する。また、画像に対して主軸方向が同一で、スライシング構造を持つ複数の長方形とする。本論文では、実用的な計算時間で高精度の長方形検出をおこなうため、次のようなさまざまな工夫をおこなっている。(1) 長方形群の主軸 2 方向に沿ったスライス処理を施すことによって、長方形が存在する可能性の高い領域を限定する処理をおこなっている。そこで得られた領域ごとに、長方形検出のためのしきい値を適応的に設定することによって、欠損率の異なる長方形を一度に検出できるようにしている。(2) ノイズカットや濃度値データの計算といった前処理を施すことによって、計算効率と検出精度の向上を図っている。(3) 線形時間の動的計画法を利用して長方形の辺候補が存在する部分を絞り込むことによって、辺候補 4 本の組合せで得られる長方形候補の数を劇的に減らし、結果として計算時間の大幅な短縮を達成している。

4. D.Z. Chen, O. Daescu, Y. Dai, N. Katoh, X. Wu:
"Efficient Algorithms and Implementations for Optimizing the Sum of Linear Fractional Functions, with Applications", Journal of Combinatorial Optimization, Vol.9 No.1, 69-90, 2005.1.
概要: The problem of optimizing the sum of m linear fractional functions (SOLF) in a fixed dimension d, subject to n linear constraints, arises in a number of theoretical and applied areas. This paper presents an improved algorithm for solving the SOLF problem in 2-D. A key subproblem to our solution is the *off-line ratio query* (OLRQ) problem, which computes the optimal values of a sequence of m linear fractional functions (called ratios), with the ratios subject to a dynamically changing feasible domain defined by $O(n)$ linear constraints. Based on useful geometric properties and the parametric linear programming technique, we develop an algorithm that solves the 2-D OLRQ problem in $O((m+n)\log(m+n))$ time. Our OLRQ algorithm can be easily implemented and is robust. More importantly, it enables us to speed up every iteration of a known iterative SOLF algorithm in 2-D, from $O(m(m+n))$ time to $O((m+n)\log(m+n))$. Implementation results of our improved SOLF algorithm have shown that in most cases our algorithm outperforms the commonly-used approaches for the SOLF problem.

5. 大崎 純, 西脇眞二:
"スナップスルーを利用したバイステーブルコンプライアントメカニズムの形状設計法", 日本機械学会論文集 A, 70(700), 23-28, 2004 年 12 月.
概要: A general approach is presented for generating compliant mechanisms from a highly connected ground structure. The structure is modeled as a pin-jointed truss, and geometrical nonlinearity is considered. An optimization problem is formulated for minimizing the total structural volume under constraints on the displacement at the specified node, and stiffnesses at initial and final states. The design variables are cross-sectional areas and the nodal coordinates. It is shown in the numerical examples that several mechanisms can be naturally found as a result of optimization starting from randomly selected initial solutions.

6. Tetsuo Asano, Naoki Katoh, Hisao Tamaki and Takeshi Tokuyama:
"The structure and number of global roundings of a graph", Theoretical Computer Science, (掲載予定).
概要: Given a connected weighted graph $G = (V, E)$, we consider a hypergraph $H_G = (V, P_G)$ corresponding to the set of all shortest paths in G. For a given real assignment $\mathbf{a}$ on V satisfying $0 \leq \mathbf{a}(v) \leq 1$, a global rounding α with respect to H_G is a binary assignment satisfying that $|\sum_{v \in F} \mathbf{a}(v) - \alpha(v)| < 1$ for every $F \in P_G$. We conjecture that there are at most $|V|+1$ global roundings for H_G, and also the set of global roundings is an affine independent set. We give several positive evidences for the conjecture.

7. Tetsuo Asano, Mark de Berg, Otfried Cheong, Hazel Everett, Herman Haverkort, Naoki Katoh, and Alexander Wolff:
"Optimal Spanners for Axis-Aligned Buildings", Computational Geometry: Theory and Applications, (掲載予定).
概要: We consider the following problem: We wish to connect buildings using bridges or tunnels, such that people can pass between the buildings without having to step outside. It is frustrating if such a connection is much longer than the direct but cold outside walk, so we want to place the bridges such that the *dilation* of the resulting network is minimum, where the di-

lation is the maximum ratio between distance within the network and beeline distance over all pairs of points in the given buildings. Given n axis-parallel rectangular buildings and a set of pairs of buildings that are to be connected by axis-parallel bridges, we can find a minimum-dilation bridge placement in $O(n^2)$ time if the building-bridge graph is a path. For the case that the graph is a tree, we give a pseudo-polynomial solution based on an LP-formulation of the problem. We show that the problem is NP-hard if the graph has cycles.

8. X. Gandibleux, H. Morita, N. Katoh:
"Population-based heuristic for solving assignment problems with two objectives", Journal of Mathematical Modelling and Algorithms, （掲載予定）.
概要: A population-based heuristic for computing an approximation of the efficient solution set for the assignment problem with two objectives is presented. The principle of the heuristic is based on an intensive use of three operators performed on a population composed only of elite solutions. The operators are a local search, a crossover and a path-relinking. The initial population is a subset of supported solutions, where each of them is one optimal assignment for an appropriate weighted sum of two objectives. A genetic information is derived from elite solutions. It is a useful genetic heritage to be exploited by crossover operators. A lower bound set defined in the objective space provides one acceptable limit for performing a local search. Results of extensive numerical experiments are reported and discussed. They show that the heuristic is able to find quickly a very good approximation of the efficient frontier and outperforms the previous results published. But also this heuristic has two main advantages; it is based on simple principles easy to implement and it does not need a tuning phase of parameter.

9. Naoki Katoh and Taihei Yano:
"An Approximation Algorithm for the Pickup and Delivery Vehicle Routing Problem on Trees", Discrete Applied Mathematics, （掲載決定）.
概要: This paper presents an approximation algorithm for a vehicle routing problem on a tree-shaped network with a single depot where there are two types of demands, pickup demand and delivery demand. Customers are located on nodes of the tree, and each customer has a positive demand of pickup and/or delivery. Demands of customers are served by a fleet of identical vehicles with unit capacity. Each vehicle can serve pickup and delivery demands. It is assumed that the demand of a customer is splittable, i.e., it can be served by more than one vehicle. The problem we are concerned with in this paper asks to find a set of tours of the vehicles with minimum total lengths. In each tour, a vehicle begins at the depot with certain amount of goods for delivery, visits a subset of the customers in order to deliver and pick up goods and returns to the depot. At any time during the tour, a vehicle must always satisfy the capacity constraint, i.e., at any time the sum of goods to be delivered and that of goods that have been picked up is not allowed to exceed the vehicle capacity. We propose a 2-approximation algorithm for the problem.

10. M. Ohsaki and S. Nishiwaki:
"Shape design of pin-jointed multi-stable compliant mechanisms by utilizing snapthrough behavior", Structural and Multidisciplinary Optimization, （掲載決定）.
概要: A general approach is presented for generating pin-jointed multi-stable compliant mechanisms utilizing snapthrough behavior. An optimization problem is

formulated for minimizing the total structural volume under constraints on the displacements at the specified nodes, stiffnesses at initial and final states, and load factors to lead to snapthrough behavior. The design variables are cross-sectional areas and the nodal coordinates. It is shown in the numerical examples that several mechanisms can be naturally found as a result of optimization starting from randomly selected initial solutions. It is also shown that no local bifurcation point exists along the equilibrium path, and the obtained mechanism is not sensitive to initial imperfections.

研究会等

1. Tetsuo Asano, Naoki Katoh, Hisao Tamaki, Takeshi Tokuyama:
"On Geometric Structure of Global Roundings for Graphs and Range Spaces", Proc. of 9th Scandinavian Workshop on Algorithm Theory, LNCS 3111, Springer, 455-467, 2004.7.
概要: Given a connected weighted graph $G = (V, E)$, we consider a hypergraph $H_G = (V, P_G)$ corresponding to the set of all shortest paths in G. For a given real assignment $\mathbf{a}$ on V satisfying $0 \leq \mathbf{a}(v) \leq 1$, a global rounding α with respect to H_G is a binary assignment satisfying that $|\sum_{v \in F} \mathbf{a}(v) - \alpha(v)| < 1$ for every $F \in P_G$. We conjecture that there are at most $|V|+1$ global roundings for H_G, and also the set of global roundings is an affine independent set. We give several positive evidences for the conjecture.

2. Danny Z. Chen, Jinhee Chun, Naoki Katoh, and Takeshi Tokuyama:
"Efficient Algorithms for Approximating a Multi-Dimensional Voxel Terrain by a Unimodal Terrain", Proc. of 10th International Computing and Combinatorics Conference(COCOON 2004), LNCS 3106, Springer, 238-248, 2004.8.
概要: Optimized region rules developed by Fukuda et al. are effective tools in data mining for a database with numeric data. However, there are two defects in the previous methods: (1) each rule can contain at most two numeric conditional attributes, and (2) the decision is only done by whether a given data is inside of a region R or outside of it, irrelevant to its exact position. In this paper, we propose a method for resolving these defects. Indeed, by applying graph algorithms, we give optimized numeric association rules with more than two attributes, and also give layered-structured numeric association rules. The method is also applicable to removal of exceptional data and also clustering.

3. N. Katoh, M. Ohsaki and Y. Xu:
"A uniform triangle mesh generation of curved surfaces", Proc. Third China-Japan-Korea Joint Symposium on Optimization of Structural and Mechanical Systems (CJK-OSM3), 759-764, 2004.11.
概要: The purpose of this study is to maximize the number of edges with almost equal lengths for a triangular mesh of a curved surface, so that the distortion of the triangulation used for finite element model or architectural latticed roofs is to be minimized. Two approximation algorithms are presented for triangulation of a polygon in a plane under upper and lower bounds on the edge lengths; (a) minimize the number of internal node, and (b) minimize the number of different edge lengths. For a parametric surface, the domain on a parametric surface is first mapped to a plane to obtain a polygon. The algorithm (b) is applied to the polygon to find a triangulation, which is remapped to the surface. The performance of the proposed method is demonstrated by using a tensor product Bézier surface.

4. Boris Aronov, Tetsuo Asano, Naoki Katoh, Kurt Mehlhorn, Takeshi Tokuyama:
"Polyline Fitting of Planar Points under Min-Sum Criteria", Proc. of 15th Symposium on Algorithms and Computations, LNCS 3341, Springer Verlag, 77-88, 2004.12.
概要: Fitting a curve of a certain type to a given set of points in the plane is a basic problem in statistics and has numerous applications. We consider fitting a polyline with k joints under the min-sum criteria with respect to L_1- and L_2-metrics, which are more appropriate measures than uniform and Hausdorff metrics in statistical context. We present efficient algorithms for the 1-joint versions of the problem, and fully polynomial-time approximation schemes for the general k-joint versions.

5. M. Ohsaki and S. Nishiwaki:
"Shape design of bistable compliant mechanisms by utilizong snapthrough behavior", Proc. Third China-Japan-Korea Joint Symposium on Optimization of Structural and Mechanical Systems (CJK-OSM3), 359-364, 2004年10月.
概要: A general approach is presented for generating compliant mechanisms from a highly connected ground structure. The structure is modeled as a pin-jointed truss, and geometrical nonlinearity is considered. An optimization problem is formulated for minimizing the total structural volume under constraints on the displacement at the specified node, and stiffnesses at initial and final states, where the design variables are cross-sectional areas and the nodal coordinates. It is shown in the numerical examples that several mechanisms can be naturally found as a result of optimization starting from randomly selected initial solutions.

6. M. Ohsaki, J. Zhang and S. Kimura:
"An Optimization Approach to Design of Geometry and Forces of Tensegrities", Int. Symposium of Shell and Spatial Strustures, (発表予定).
概要: A general method is presented for direct design of member directions, force vectors and nodal locations of tensegrities with given topology, which is defined as a directed graph. The system of equilibrium equations is written in terms of the components of the member force vectors by using the incidence matrix. Since the number of the total components of the force vectors is usually larger than the rank of the equilibrium matrix, some force components can be arbitrary specified. The target values are given here to formulate an optimization problem to obtain a set of force components that satisfies equilibrium conditions. By using the proposed method, the designers can directly control the axial forces and the configuration simultaneously, which is considered a major advantage of the method. A new configuration can also be obtained by changing the target values of the forces and geometrical constraints.

7. J. Zhang and M. Ohsaki:
"Form-finding of Self-stressed Structures by an Extended Force Density Method", Int. Symposium of Shell and Spatial Strustures, (発表予定).
概要: The force density method is extended to find the feasible set of force densities, based on singular value decomposition of equilibrium matrix, and an algorithm for specifying an independent set of nodal coordinates is proposed. The force densities is first formulated in terms of elements of the equilibrium matrix, where constraints on force densities with desired values can be included at the same time. The least square solution of the force densities is then given based on this formulation. Singu-

lar value decomposition is next applied to the equilibrium matrix and its smallest elements with the specified number are set to be zero in order to attain the required rank. The equilibrium matrix is reconstructed for calculation of force densities by the equations formulated previously. By iteratively carrying out the above processes of calculating force density vector and equilibrium matrix with the updated ones, a feasible set of force densities is derived. The last step of the method is to specify an independent set of nodal coordinates to achieve a unique geometrical configuration of the structure.

8. M. Ohsaki and N. Katoh:
"Topology optimization of trusses with stress and local constraints", Int. Conference on Computation of Shell and Spatial Structures, (発表予定).
概要: A mixed integer programming formulation is presented for the truss topology optimization with stress and local constraints. Linear programming problems are successively solved based on a branch-and-bound method, where an upper-bound solution is obtained by solving nonlinear programming problems. It is shown in the examples that upper- and lower-bound solutions with small objective gap can be found, and the computational cost can be reduced by utilizing the local constraints.

学会大会等

1. 加藤直樹，宮高泰匡，瀧澤重志:
"建築画像のデータベースに対する自動索引付けのための建築構成要素の認識手法の開発　畳と格子を例として", 日本建築学会大会学術講演梗概集, A-2, pp.539-540, 2004.

2. 神山直行，瀧澤重志，加藤直樹:
"フロアプラン列挙に基づく二層構造物の室配置最適化手法", 日本建築学会大会学術講演梗概集, A-2, pp.559-560, 2004.

3. 大崎 純，西脇眞二:
"スナップスルーを利用したバイステーブルコンプライアントメカニズムの形状設計法", 計算工学講演会論文集, 9, 399-402, 2004 年 5 月.

4. M. Ohsaki:
"Multiple eigenvalues in topology optimization", International Workshops on Advances in Computational Mechanics, 114, 2004 年 11 月.

5. 大崎 純，西脇眞二:
"バイステーブルコンプライアントメカニズムの形状設計と不整感度解析", 第 6 回最適化シンポジウム講演論文集，日本機械学会, 257-262, 2004 年 12 月.

6. 塚本智久，川口史恵，加藤直樹，瀧澤重志:
"都市における線的施設配置問題に関する研究", 日本建築学会近畿支部研究報告集, (発表予定).

7. 瀧澤重志:
"不整形な宅地分割を意図した区画割と道路配置の同時最適化に関する基礎研究", 日本建築学会近畿支部研究報告集, (発表予定).

A07: 現実的な状況下での量子計算の能力に関する研究

山下 茂　中西 正樹

奈良先端科学技術大学院大学 情報科学研究科
〒 630-0192 奈良県生駒市高山町 8916-5
{ger, m-naka}@is.naist.jp

1　はじめに

量子計算の計算機科学からの研究は，量子チューリングマシンと呼ばれる非常に理想的な量子計算機のモデルの上で，計算ステップ数の漸近的な評価をしているものがほとんどである．本研究では，より現実的な状況を考慮して，量子計算の一部分が古典的な計算資源で置き換えられたり，量子計算の一部分がエラーを含んだりする場合などのモデルにおいて，量子計算の計算能力の解析を行なうことを目的としている．また，計算の大部分を古典計算機で行なわなければならないような現実的な状況において，量子計算機を利用すれば，古典計算だけの場合よりもより高速に解ける問題やその状況，およびその具体的な利用方法についての知見を得ることも目標としている．本年度は，この目標に対して以下のような研究を行なった．

古典スタック付き量子プッシュダウンオートマトンの計算能力

量子デバイスと古典デバイスが協調して動作する計算機のモデルとして古典スタック付き量子プッシュダウンオートマトンを提案し，片側誤りのもとで純粋な古典モデルより真に能力が高いことを示した．

エラーのある量子オラクルの分類を行う量子アルゴリズム

ある決められたオラクルの集合が与えられ，そのうちの一つがブラックボックスとして与えられた時に，何回そのブラックボックスのオラクルに質問すれば，オラクルを同定できるかという問題をオラクル同定問題という．オラクルが量子的なサブルーチンとして Grover Search に利用できる時に，たとえオラクルが定数確率で間違った値を返す場合でも，エラーがない場合の問い合わせ回数の下限と一致するオラクルへの問い合わせ回数でオラクル同定問題を解く量子アルゴリズムを設計した．

N 個の関数の値の OR を分散環境で効率よく計算する量子プロトコル

Alice と Bob が l 個の入力データ x と y をそれぞれ持っている状況で，l 個の $f(x,y)$ の出力の OR を計算するときに Alice と Bob の間で必要な通信量（ビット数）を考える．特に，f が $x \neq y$ かどうかをチェックする関数のとき，この問題は list-nonequality function:$LNE(l,k)$ と呼ばれ，分散環境での通信量に関して基本的な問題である．この問題に対して，量子のプロトコルに古典のランダムコインの概念をうまく取り入れることによって，古典の場合よりも効率的な計算手法を設計した．

古典計算機と量子計算機を協調させてプログラミングする枠組み

通常の C++で書かれたプログラムからほぼ全自動で，Grover Search で置き換えていい部分を判定し，その量子アルゴリズムに相当する量子回路を生成する手法を実現した．今後は Grover Search 以外の量子アルゴリズムについても検討する課題が残っている．

以下では，それぞれの研究項目についてその概要を述べる．

2 古典スタック付き量子プッシュダウンオートマトンの計算能力

シンプルな量子計算機のモデルとして，量子有限オートマトンや，量子プッシュダウンオートマトンが提案されている．特に量子有限オートマトンは量子チューリング機械や量子回路と異なり，必要な量子資源が有限であるため，現実的に実現できる量子計算機の規模を考えると，非常に重要なモデルである．

一方，計算機のすべてを量子デバイスを用いて実装するのは現実的ではない．量子計算機が実現した場合は，少ないメモリしか持たない量子計算機と多くのメモリを持つ古典計算機を協調して動作させることが必要となる．シンプルな量子計算機と古典計算機が協調して動作した場合，量子計算機単独で動作するよりも能力が高くなる場合がある．

そこで，本研究ではこのような量子デバイスと古典デバイスが協調して動作するような計算機の能力の解析を行った．量子デバイスと古典デバイスが協調して動作するモデルを考えることは，上述の理由の他に，可逆性を緩和できるという利点がある．量子計算モデルは量子力学から来る制約上，可逆な計算モデルでなければならない．この制約は場合によっては量子計算モデルの能力を古典計算モデルより弱くすることにもなりうる．しかしながら，古典デバイスはこのような可逆性という制約を受けないため，自由に操作ができる．

本研究では，計算モデルとしてプッシュダウンオートマトンを考え，その有限状態制御部とテープヘッドに量子デバイスを，スタックに古典デバイスを用いた量子-古典協調計算モデルを提案し，その能力の解析を行った．結果として，片側誤りのもとで，量子計算モデルの方が古典計算モデルよりも認識できる言語のクラスが大きくなる，つまり，能力が高くなることを示した．

以下に，本研究で提案した古典スタック付き量子プッシュダウンオートマトンの定義を与える．

Definition 1 古典スタック付き量子プッシュダウンオートマトンは次の *8* 項組で定義される．

$$M = (Q, \Sigma, \Gamma, \delta, q_0, \sigma, Q_{acc}, Q_{rej}),$$

ここで Q は状態の有限集合, Σ は左 *(*右*)* 終端記号 $\not\vdash$ *(*\$*)* を含む入力アルファベット，Γ は底記号 Z を含むスタックアルファベット，$\delta : (Q \times \Sigma \times \Gamma \times Q \times \{0,1\}) \longrightarrow \mathbb{C}$ は状態遷移関数，q_0 は初期状態，$\sigma : Q \setminus (Q_{acc} \cup Q_{rej}) \longrightarrow \Gamma^+ \cup \{-, pop\}$ はスタック操作を決める関数，Q_{acc} $(\subseteq Q)$ は受理状態集合， Q_{rej} $(\subseteq Q)$ は非受理状態集合である．ただし，$Q_{acc} \cap Q_{rej} = \emptyset$ とする．

□

このモデルは，量子有限オートマトンに古典のスタックを付加したものと考えることができ，量子有限オートマトン部の動作は，スタックトップの記号に基づいて決められるユニタリ変換によって規定される．また，スタックの操作は量子有限オートマトン部の観測結果に基づいて積むべき記号 (あるいはスタックトップの削除) が決定される．具体的には次のように動作を行う．

$\delta(q, b, a, q', D) = \alpha$ は状態 q で入力記号 b，スタック記号 a を読んだときに状態 q' に遷移して，ヘッドを D の方向に動かす確率振幅が α であることを示している．状態 q，ヘッド位置 k に対する時点表示を $|q, k\rangle$ と表すと，古典スタック付き量子プッシュダウンオートマトンの (量子有限状態制御部の) 1 ステップの動作は次のようにユニタリ変換 $U_a^{\boldsymbol{x}}$ を適用することに相当する．ここで，a はスタックトップの記号，$\boldsymbol{x}$ は入力文字列を表すものとする．

$$U_a^{\boldsymbol{x}}(|q, k\rangle) = \sum_{q' \in Q, D \in \{0,1\}} \delta(q, x(k), a, q', D) \left|q', k + D\right\rangle,$$

ここで，$x(k)$ は 入力文字列 $\boldsymbol{x}$ の k 番目の入力記号を表すものとする．

量子有限状態制御部に対して，ユニタリ変換 $U_a^{\boldsymbol{x}}$ が適用された後，次に示す観測量を用いて観測が行われる．

$$\begin{aligned} E_w &= span\{|q, k\rangle \,|\sigma(q) = w\}, \\ E_{\mathrm{acc}} &= span\{|q, k\rangle \,|q \in Q_{\mathrm{acc}}\}, \\ E_{\mathrm{rej}} &= span\{|q, k\rangle \,|q \in Q_{\mathrm{rej}}\}. \end{aligned}$$

と定め，観測量を $\mathcal{O} = \oplus_j E_j$ と定義する．

観測の結果が acc (rej) であれば，入力を受理 (非受理) する．観測の結果が pop であれば，ス

タックトップ記号をポップする．‘–’ であればスタックを変化させない．それ以外の場合 (つまり，j が Γ^+ の文字列の場合) は j をスタックにプッシュする．以上を繰り返すことにより，計算を進める．

本研究では，古典スタック付き量子プッシュダウンオートマトンで片側誤りで認識できるが，(古典の) 確率プッシュダウンオートマトンでは片側誤りで認識できない言語が存在することを示した．

Theorem 1 次に示す言語 L_1 は古典スタック付き量子プッシュダウンオートマトンで片側誤りで認識できる．

$$L_1 = \left\{ u\#v\natural w\flat x\%y \;\middle|\; \begin{array}{l} u,v,w,x,y \in \{a,b\}^*, \\ \neg \left(\begin{array}{l} |u| = |v| = |w| = |x| \\ and\ v = w \end{array} \right) \\ and \neg \left(\begin{array}{l} |u| = |x|\ and \\ |v| = |w| = 0 \end{array} \right) \\ and\ (y = v^R\ or\ y = w^R) \end{array} \right\}$$

□

Theorem 2 L_1 は文脈自由言語ではない．

□

定理 2 より，L_1 は非決定性プッシュダウンオートマトンで認識できないことがわかる．片側誤り確率プッシュダウンオートマトンが認識できる言語のクラスは，非決定性のそれより真に小さいことに注意すると，L_1 は片側誤り確率プッシュダウンオートマトンで認識できないことがわかる．

著者らは今までに任意の確率プッシュダウンオートマトンは同じ確率で入力を受理する可逆確率プッシュダウンオートマトンに変換できることを示している．

Theorem 3 可逆確率プッシュダウンオートマトンは任意の確率プッシュダウンオートマトンを同じ確率で入力を受理するようにシミュレートすることができる．

□

定理 3 より，任意の確率プッシュダウンオートマトンは量子プッシュダウンオートマトンでシミュレート可能であることが言える．このことと定理 1，2 を合わせると，古典スタック付き量子プッシュダウンオートマトンは片側誤りのもとで，確率プッシュダウンオートマトンより真に能力が高いことが言える．

3 エラーのある量子オラクルの分類を行う量子アルゴリズム

Grover の探索アルゴリズムなどのオラクルを用いて解く問題の一般化として，以下のようなオラクル同定問題というものが考えられている．

オラクル同定問題

入力： M 個のオラクル集合 $S = \{f_1, ..., f_M\}$ とその中のオラクル $f_i : \{0,1\}^n \to \{0,1\},\ f_i \in S$.

出力： オラクル f_i のインデックス i.

解が一つの場合の探索問題（つまりオラクル $f_i(i) = 1, f_i(j) = 0\ (j \neq i)$ から i を求める Grover の探索問題），およびビット毎の積の論理和（内積）$f_i(j) = i \cdot j$ から i を求める問題もオラクル同定問題の一例である．言い替えると，オラクル同定問題は，M 個のオラクルの動作がわかっているという条件で，ブラックボックスにその内の一つが隠されている時に，オラクルへのクエリーを用いてどのオラクルがブラックボックスに隠されているかを決定する問題である．これは，$M \times N$ 行列 $(N = 2^n, N \leq M \leq 2^N)$ が与えられ，現在のオラクル（ブラックスボックスに隠されたオラクル）がどの行であるかを同定する問題と見ることもできる．そのため，以下では，「$M \times N$ 行列に対するオラクル同定問題」と呼ぶことにする．

オラクル同定問題において，オラクルがエラーを持つ場合に，エラー除去のために増加するクエリー回数が定数倍程度で済む量子アルゴリズムを以下で述べる．ここでは，$M = N$，すなわちオラクル候補の数がオラクル入力の長さと一致する場合を考える．(Grover の探索アルゴリズムの問題もこの場合に相当する．)

エラー付きオラクル同定問題

入力： M 個のオラクル集合 $S = \{f_1, ..., f_M\}$ とその中のある一つのオラクル $f_i \in S$ を計算するユニタリ変換 U_{f_i}:

$$U_{f_i} |x\rangle |0\rangle |0\rangle =$$

$$\sqrt{p_x} |x\rangle |\phi_i\rangle |f_i(x)\rangle + \sqrt{1-p_x} |i\rangle |\psi_i\rangle |\neg f_i(x)\rangle ,$$

但しある定数 $0 < \varepsilon < 1/2$ に対して，$1/2 + \varepsilon \leq p_x^2 \leq 1$ である．

出力： オラクル f_i のインデックス i.

エラー無しの場合は，$O(\sqrt{N})$ 回のオラクルクエリーにより解けることが既に知られている．しかし，このアルゴリズムは古典的なオラクルクエリーを数多く利用しているために単純に頑健な量子探索アルゴリズムを利用するするだけでは，$O(\log N)$ 倍のオラクルクエリーが避けられない．そのため，エラーがあるオラクルの同定問題をエラーのない場合に対して定数倍程度のクエリー回数の増加で解く量子アルゴリズムは自明でない．しかし，実際には以下の定理が成り立つ．

Theorem 4 $N \times N$ 行列に対するエラー付きオラクル同定問題を $O(\sqrt{N})$ 回のオラクルクエリーにより少なくとも定数確率で解くアルゴリズムが構成可能である． □

ここでは，アルゴリズムを簡単に述べる．

1. 以下の 2.–6. をオラクル候補 Z が一つになるまで繰り返す．最初 は Z を与えられた N 個のオラクル候補全てとする．

2. 以下の操作では，Z の各列に対して**列反転** (column flip) を行う．ここで列反転とは Z の各列において，もし 1 が 0 の数より少なければ，その列の 0,1 を反転し，そうでなければそのままにしておく，という操作である．この操作で各列での 1 の数が 0 の数よりも少ない行列として常に扱うようにする．(この操作にはクエリーを全く用いないことに注意する.)

3. 以下の 4. を選択された列によって**被覆**された行が $|Z|/3$ を超えるまで，あるいは選択する列がなくなるまで繰り返す．ここで列 j が行 i を被覆するとは $f_i(j) = 1$ を満たす，つまり i 行 j 列が 1 であることを意味する．最初，選択された列の集合 T は空集合とする．

4. T に属する列で被覆されていない行において 1 の数が最大の列を選び，T で被覆されてない行のうち $\sqrt{|Z|}/\log N$ 行を被覆しているならば，それを T に含める．

5. T に属する列に対して頑健な量子探索アルゴリズムを $O(\log N)$ 回適用する．1 が発見できれば T が被覆する行を新たに Z とおいて 2. へ戻る．

6. 5. で 1 が発見できなかった場合，以下のいずれかを行なう．

6.a T で被覆する行数が $|Z|/3$ 以上だった場合，T が被覆する行を除外したものを新たに Z として 2. に戻る．

6.b T で被覆する行数が $|Z|/3$ 未満だった場合，T が被覆する行を除外した行列に対して 7.-9. を実行する．

7. T に属さない列に対して頑健な量子探索アルゴリズムを適用する．

8. T に被覆されていない列の中で，7. で得られた列に 1 を持つ行を選ぶ．選ばれた行の集合を S' とする．

9. T に被覆されていない列の中で，S' 中に 0 と 1 両方含んだ列を探し，$\log N$ 回の古典的クエリーでその列の値を決定し，その結果に矛盾する行を Z から削除する．7.–9. を $|Z| = 1$ になるまで繰り返す．

上記のアルゴリズムに対して，オラクルのクエリー回数を評価する．5. で必要なクエリー回数は $O(\sqrt{|T|}\log N)$ であるが，$|T| \leq |Z|/(\sqrt{|Z|}/\log N) = \sqrt{|Z|}\log N$ より，5. で 1 が発見できた場合にはクエリー回数 $O(|Z|^{1/4}\log^{3/2} N)$ で確率 $1 - O(1/N)$ でオラクル候補の総数を 1/2 以下に絞り込むことができることになる．一方，5. で 1 が発見できなかった場合には，確率 $1 - O(1/N)$ 以上でオラクルは T に属さないことになる．従って，T が被覆する行数が $|Z|/3$ 以上だった場合には，オラク

ル候補の総数を 2/3 以下に絞り込むことができる．また，T が被覆する行数が $|Z|/3$ 未満だった場合には T で被覆された行を除外した後の各列に含まれる 1 の数が $\sqrt{N}/\log N$ という事実に注目すると 7.–9. で $\log N$ 回のクエリーをせいぜい $\sqrt{N}/\log N$ 回繰り返せばよい．よってこのときのクエリー回数は $O(\sqrt{N})$ 回である．従って全体でせいぜい $O(N^{1/4}\log^{5/2} N + \sqrt{N}) = O(\sqrt{N})$ のクエリー回数でオラクル同定が定数確率で可能である．

このアルゴリズムを改良して，さらに以下のことを示した．アルゴリズムが複雑なためここでは，結果のみを示す．

Theorem 5 $M\times N$ 行列に対するエラー付きオラクル同定問題を $M = poly(N)$ の時には，$O(\sqrt{N})$ 回のオラクルクエリーにより，少なくとも定数確率で解くアルゴリズムが構成可能である． □

Theorem 6 $M \times N$ 行列に対するエラー付きオラクル同定問題を $poly(N) \leq M \leq 2^{N^d}$ *(*d は $0 < d < 1$ の定数*)* の時には，$O(\sqrt{N\frac{\log M}{\log N}})$ 回のオラクルクエリーにより，少なくとも定数確率で解くアルゴリズムが構成可能である． □

オラクルにエラーがない場合でも，$M\times N$ 行列に対する同定問題のオラクルクエリーの下限が，$\Omega(\sqrt{N\frac{\log M}{\log N}})$ であることが既に示されているので，本研究の結果はほぼ最適であることがわかる．

4 N 個の関数の値のＯＲを分散環境で効率よく計算する量子プロトコル

Alice と Bob がネットワークでつながっていて，Alice が k ビットの入力 x を持ち，Bob が k ビットの入力 y を持っているとする．この状況で，x と y からある関数 $f(x,y)$ を計算するのに Alice と Bob の間で何ビットのデータ (通信量) をやり取りしなければならないかという問題は，分散環境において行う計算の効率を考える上での基本的な問題である．この応用で，Alice と Bob が l 個の入力データを持っている状況で，l 個の f の出力のＯＲ ($f^{\vee l}$ と表記する) を計算する問題に必要な通信量に関しても（古典）計算量の分野では多く研究されている．

本研究では，量子計算機が使える状況，すなわち，ネットワークと計算機が量子情報を扱える場合に，上記の問題を解く効率的な量子分散アルゴリズムが構築できることを示した．その手法は，古典のテクニックとして用いられる共通のコイン（乱数）を用いるモデルを拡張し，古典のコインを用いる量子計算のモデルを構築することを基本としている．特に f が $x \neq y$ かどうかをチェックする関数のとき，上記の問題は list-nonequality function: $LNE(l,k)$ と呼ばれる．古典計算の状況では LNE を解くのに必要な通信量は，$\Theta(l+\log k)$ であることがわかっているが，本研究で構築した量子アルゴリズムでは $O((\sqrt{l}\log l+\log k)$ で解けるため，古典計算より効率が良いことが分かる．

本研究の成果を述べる前に，Høyer らが示した再帰的に Amplitude Amplification を適用して INT_n を解く量子プロトコルを単純に応用した，量子プロトコルについて述べる．

Theorem 7 f を $f:\{0,1\}^k\times\{0,1\}^k \longrightarrow \{0,1\}$ であるような任意の関数，$\mathcal{P}$ を f を有界誤りで計算する量子通信プロトコルであるとする．このとき，ある定数 c に対して $Q_2(f^{\vee l}) = O(c^{\log^* l}\sqrt{l}\cdot C(\mathcal{P}))$ となる．ここで $C(\mathcal{P})$ はプロトコル $\mathcal{P}$ のコストを表すものとする． □

これより，$\overline{\mathrm{LNE}(l,k)} = \bigvee_{i=1}^{l} EQ_k$ であり，かつ，$Q_2(EQ_k) = \Theta(\log k)$ であることを考慮して，以下の Corollary を得る．

Corollary 1 $Q_2(LNE(l,k)) = O(c^{\log^* l}\sqrt{l}\cdot\log k)$. □

古典通信プロトコルの場合，共通コインを用いたプロトコルを基に，共通コインを用いないプロトコルを構築することができる．したがって，基となる共通コインを用いるプロトコルとして，効率が良いものを考えることにより，効率のよい (共通コインを用いない) プロトコルを構築することが可能である．具体的には，共通コインを用いた f を計算するプロトコルを基に共通コインを用いた $f^{\vee l}$ を計算するプロトコルを構築し，次に，このプロトコルを $O(\log lk)$ ビットの通信を付加することで共通コインを用いないプロトコル

に変換する．ここで k は f の入力長，つまり，Alice と Bob の持つ入力のサイズは $O(lk)$ である．ここで，使用した共通コインの個数に関わらず，必要となる付加的な通信量は $O(\log lk)$ であることに注意されたい．この手法を用いることにより，$\mathrm{LNE}(l,k) = \overline{\mathrm{EQ}_k^{\vee l}}$ の古典有界誤りプロトコルの通信量は，$\Theta(l+\log k)$ となる．したがって，Corollay 1 で示した量子プロトコルは必ずしも古典のプロトコルより効率的であるとは限らない．

このことを踏まえ，本研究では上述の手法を量子プロトコルに適用し，定理 7 の結果を改良する方法を示した．つまり，再帰の基底プロトコルとして EQ_k を計算する通信量 $O(1)$ の (古典) 共通コインを用いるプロトコルを用いた $\mathrm{LNE}(l,k)$ のプロトコルを考え，上述の手法により $O(\log lk)$ ビットの通信を付加して，共通コインを用いないプロトコルに変換する．これにより，古典の通信量 $\Theta(l+\log k)$ より常に少ない通信量を実現する量子プロトコルを構築することができる．しかしながら，量子プロトコル中で古典の共通コインを用いるため，上述の手法が単純に量子プロトコルに適用できるかは自明ではない．実際，古典コインを用いた量子プロトコルを構築するにはいくつかの問題点に注意を払う必要がある．この問題点を取り扱うために以下にいくつかの定義を行う．

Definition 2 任意の個数の古典共通コインを使用できる量子プロトコルを古典共通コイン量子プロトコルと呼ぶ．$Q_2^{pub}(f)$ を f を計算する有界誤り古典共通コイン量子プロトコルのコストのうち最小のものとする． □

上述の定義では，重ね合わせ中の基底それぞれについて，異なる古典コインを参照することができる．したがって，十分な個数の古典コインをあらかじめ用意しておく必要がある．ここで，古典共通コインプロトコルは古典共通コイン量子プロトコルに変換できることに注意されたい．しかしながら，たとえ定理 7 のプロトコルに古典共通コインを導入したとしても上述の変換手法に基づいて，ある定数 c_1，c_2 に対して，$Q_2(f^{\vee l}) = O(c_1^{\log^* l}\sqrt{l}R_2^{pub}(f) + \log k)$ となるような古典のプロトコルよりも常に効率の良い古典共通コイン量子プロトコルを構築できるとは限らない．これは以下のような理由による．量子振幅増幅アルゴリズムは純粋状態に対して適用可能なアルゴリズムである．つまり，次のような変換をおこなう．$\mathcal{A}|0^m\rangle = \alpha|\psi_{good}\rangle + \sqrt{1-\alpha^2}|\psi_{bad}\rangle$．ここで $\mathcal{A}$ は成功確率を増幅したいアルゴリズム (プロトコル) を表す．しかしながら，古典共通コイン量子プロトコルは (古典の) 確率にしたがうプロトコルであるため，量子状態は純粋状態でなく混合状態として記述される．したがって，単純に量子振幅増幅アルゴリズムを適用することができなくなる．

そこで，混合状態に量子振幅増幅アルゴリズムを適用するための手法が必要になる．以下では，このためにいくつかの準備を行う．

Definition 3 *(*古典共通コイン*)* 量子プロトコル $\mathcal{P}$ はプロトコル実行後の状態が確率 p で $|\psi\rangle = \alpha|\psi_{good}\rangle + \beta|\psi_{bad}\rangle$ と書けるとき， 確率 p で関数 f を純粋状態において有界誤りで解くという．ここで， $|\alpha|^2 > \frac{2}{3}$ かつ，$|\psi_{good}\rangle$ *(*$|\psi_{bad}\rangle$*)* は正しい *(*間違いの*)* 答えが解答ビットに書かれているような状態で張られる部分空間の要素である． □

これらの定義に基づいて，本研究では以下のことを示した．

Lemma 1 $\mathcal{P}$ を f を計算する有界誤り古典共通コイン量子プロトコルとする．また，$C(\mathcal{P})$ でプロトコル $\mathcal{P}$ のコストを表すとする．このとき，少なくとも $1-\frac{\varepsilon}{l}$ の確率で f を純粋状態において有界誤りで計算する量子プロトコル $\mathcal{P}_f^{maj}$ を構築ことができる．ただし，$C(\mathcal{P}_f^{maj}) = O(\log l \cdot C(\mathcal{P}_f))$ とする． □

次に，古典通信量のモデルでの議論と同じように，古典共通コイン量子プロトコルにおいても，わずかな通信量を付加することにより共通コインを取り除くことができることを説明する．量子モデルに古典のコインを導入しているため，古典モデルにおける手法をそのまま適用できるかどうかは自明ではない．しかし，実際には古典の場合とほぼ同様の以下の結果を示すことができる．

Lemma 2 f を $f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$ なる関数とする．任意の δ，ϵ について，f を計算する任意の ϵ-誤り古典共通コイン量子プロトコルは $O(\log n + \log 1/\delta)$ ビットの通信を付加することにより，$(\epsilon+\delta)$-誤り量子プロトコルに変換できる． □

以上より，本研究における以下の主定理が示される．

Theorem 8 f を $f:\{0,1\}^k\times\{0,1\}^k \longrightarrow \{0,1\}$ なる任意の関数とする．このとき $Q_2(f^{\vee l}) = O(\sqrt{l}\cdot\log l\cdot Q_2^{pub}(f)+\log k)$.

Proof. 関数 $f^{\vee l}$ を計算する通信量が $O(\sqrt{l}\cdot\log l\cdot Q_2^{pub}(f)+\log k)$ の有界誤り量子プロトコルを以下に示す．

以下に示すプロトコルは，Høyer らの頑健な量子探索アルゴリズムに基づくものである．頑健な量子探索アルゴリズムにより，次のことが言える．「もし，f を純粋状態において有界誤りで計算する量子プロトコル $\mathcal{P}$ が存在すれば，$\mathcal{P}$ を $O(\sqrt{l})$ 適用することにより $f^{\vee l}$ を有界誤りで計算することができる．」

$\mathcal{P}_f$ を f を計算する古典共通コイン量子プロトコルとする．Lemma 1 より $\mathcal{P}_f$ を $O(\log l)$ 回適用することで，少なくとも $1-\frac{\varepsilon}{l}$ の確率で純粋状態において有界誤りで f を計算する量子プロトコル $\mathcal{P}_f^{maj}$ を構築することができる．よって，「l 個の入力に対する $\mathcal{P}_f^{maj}$ の試行がすべて純粋状態において有界誤りで関数 f を計算する」ということを少なくとも定数確率でできる．したがって，頑健な量子探索アルゴリズムを l 個の結果に対して適用することにより，全体としての成功確率が少なくとも定数になる．

l 個の入力に対して，プロトコル $\mathcal{P}_f^{maj}$ を量子重ね合わせの状態で適用する際，何番目の入力に対してプロトコルを実行すべきかという情報を Alice と Bob で交換する必要がある．この際 $O(\log l)$ ビットの通信が必要になる．したがって，全体としての通信量は $O(\sqrt{l}\cdot(\log l\cdot Q_2^{pub}(f)+\log l))(=O(\sqrt{l}\cdot\log l\cdot Q_2^{pub}(f)))$ となる．

頑健な量子探索アルゴリズム中で，S_0 と呼ばれる $|00\cdots0\rangle$ に対する位相を反転する操作を行う必要がある．この操作には定数個のビットの通信で十分であることに注意されたい．

上記のプロトコルは古典共通コインを用いているが，Lemma 2 より，共通コインを使用しないプロトコルに変換可能である．この変換により，定理中に示した通信量のプロトコルが得られる．

□

最後に，$R_2^{pub}(EQ_k)=O(1)$ であることを利用して，LNE(l,k) に対する量子プロトコルとして，常に古典プロトコル (通信量 $\Theta(l+\log k)$) よりも効率の良いものを与える．

Corollary 2 $Q_2(LNE(l,k)) = O(\sqrt{l}\cdot\log l+\log k)$. □

以上より，本研究は，非常に効率が良い古典プロトコルが知られている LNE に対して，更により効率的な量子プロトコルを示したことになる．

5 古典計算機と量子計算機を協調させてプログラミングする枠組み

現在知られている汎用的な量子アルゴリズムは，データベースサーチ（ある条件を満たすものを探すこと）を高速に行う Grover Search と呼ばれるものしかない．そのため，Grover Search を使って通常のプログラミングをどのように行うのか（すなわちどのようなプログラミング言語を用いるのか）が実用的には非常に重要となる．そこで，C＋＋の通常の記述から Grover Search にすれば効率が良い部分をどのようにして切り出すべきかの検討を行った．既存の研究としては，量子計算向けのプログラミング言語を独自に提案しているものがあるが，本研究で提案する方法は，以下で述べるとおり，より現実的であると考えられる．その概要は以下の通りである．

1. プログラムはC＋＋プログラミング言語とまったく互換の言語で記述する．

2. プログラマが，if 文でチェックをして何かを探したい場合に，それを確率的におこなってもいいと考える場合には，その直前にC＋＋のコメント文で，//Quantum Search と記述する．また，最終的に達成してほしいエラー確率をその後に記述する．(図 2.1 の例を参照)

3. システム側はその部分を量子計算機を用いた場合のオーバーヘッドを考慮して Grove Search で行うべきかを自動で判定し，指定されたエラー率を達成するだけの繰り返しの分も含めて量子回路を生成する．また，古典

```
for(int i = 0; i<10000;i++){
   //Quantum Search 0.01
  if(Data1[i] == 100) {
     return i;
  }
}
```

図 2.1: C＋＋での記述例

計算機からの呼び出しインターフェースも自動で生成する．

4. Grover Search をC＋＋でシミュレーションするサブルーチン関数も用意しておき，その関数への引数を自動生成する．(そのため実際の量子計算機を用いなくても，時間はかかるが通常のC＋＋の環境でも実行結果を検証可能となる．)

ある探索が確率的でいいかどうかはプログラマにしか分からないため，確率的に動作する Grover Search を使用可能かどうかを自動で判定するのは現実的には不可能である．そのため，上述した 2. でのディレクティブを用いた指定はプログラマへの必要最小限の負担であり，現実的な解決方法である考えている．それ以外の作業は，すべてシステム側で判断する．具体的には，該当部分を量子計算機で行うと計算時間が早くなるかどうかを，その量子回路のサイズを見積もることにより自動で判断する．考案した枠組みは，特殊な量子プログラミング言語を用いる手法に比べて以下のような利点がある．

- プログラマは通常のC＋＋で記述でき，量子計算で行ってもよいと考えるところをディレクティブで指定するだけで，あとはシステムが自動で量子計算でやらすべきかを判断してくれる．つまり，プログラマが量子計算の詳細を知らなくても，プログラミング環境が自動的に量子計算機で実行すべき部分を切り出してくれる．
- 全体がC＋＋で記述され，また，量子計算で実行される Grover Search をC＋＋でシミュレーションするライブラリもあるため，プログラム全体を既存のC＋＋コンパイラの環境でシミュレーション可能である．量子計算と古典計算を協調させてプログラムを実行させる様子を見たい場合，従来のような特殊な量子回路シミュレータしかない場合には，そのシミュレーション結果と通常のC＋＋プログラムの出力を組み合わせてシミュレーションするしか方法がない．考案した枠組みでは，特別な量子回路シミュレータを使うことなく，全体の計算を簡単にシミュレーション可能である．

以上の利点から，考案した手法は，将来の量子計算の利用の仕方として有効な手法となりうると考えられる．

上述した枠組みでは，Grover Search をすべき部分を切り出した後，それを基本ゲートによる量子回路として実現しなければいけない．従来，量子アルゴリズムを表現するユニタリ行列を行列分解により基本ゲートに分解する手法が多く提案されているが，大規模な Grover Search を表現するユニタリ行列はそれ自身が探索問題のサイズに対して指数的に大きくなるので，行列を表現して分解する手法は実用的なサイズの Grover Search には適用できない．そこで，本研究では，Grover Search の量子特有の操作で問題ごとに変化しない部分はテンプレートを用いることとし，問題ごとに変わる if の中の制御論理のみを行列分解とは違う手法で設計することを特徴としている．if(Data1[i] == 100) というような単純な場合にはこの制御論理の設計はほぼ自明だが，この部分が i の複雑な算術式で書かれていた場合それを量子回路で実現するのは自明ではない．今年度は，i の複雑な算術式で書かれている条件を，ブール関数で表現する効率的な手法を考案し，それをプログラムとして実装した．作成したプログラムを用いれば，今まで全く知られていなかった，大規模な Grover Search を実際に量子計算で行ったときの詳細な計算ステップを見積もることができるようになるため，多くの研究者に有益なツールとなると考えられる．

研究業績一覧

学術論文

1. M. Nakanishi:
   "On the Power of One-Sided Error Quantum Pushdown Automata with Classical Stack Operations", Proc. of 10th Annual International Computing and Combinatorics Conference (COCOON 2004), LNCS 3106, pp. 179–187, 2004年8月.
   概要: One of important questions on quantum computing is whether there is a computational gap between the models that are allowed to use quantum effects and the models that are not. Several types of quantum computation models have been proposed, including quantum finite automata and quantum pushdown automata (with quantum pushdown stack). It has been shown that some quantum computation models are more powerful than classical counterparts and some are not since quantum computation models are required to obey some restrictions such as reversible state transitions. In this paper, we investigate the power of quantum pushdown automata whose stack is assumed to be implemented as a classical device, and show that they are strictly more powerful than classical counterparts in the one-sided error setting. That is, we show that there is a non-context-free language which quantum pushdown automata with classical stack operations can recognize with one-sided error.

2. S. Yamashita, M. Nakanishi, K. Watanabe:
   "Toward a Practical Environment for Quantum Programming", Proc. of Asia-Pacific Conference on Quantum Information Science, (掲載予定).
   概要: This paper proposes a practical framework for quantum programming. In our framework, the parts of a program to be performed on a quantum computer are almost automatically determined, and the other parts are performed on a classical computer. We only consider Grover Search to be performed on a quantum computer in the framework because the other quantum algorithms known so far cannot be applied to general cases. By considering only Grover Search, we have several advantages that show our framework is really practical.

3. K. Iwama, A. Kawachi, R. Raymond H.P., S. Yamashita:
   "Robust Quantum Algorithms for Oracle Identification", Workshop on Quantum Information Processing 2005, Poster Presentation.
   概要: In this paper, we treat a general problem, called the *oracle identification problem (OIP)*, introduced by Ambainis et al., (STACS 04). An OIP is, given an oracle $f_i : \{0,1\}^n \rightarrow \{0,1\}$ and a candidate set $S = \{f_1, ..., f_M\}$, to determine which oracle in S is now in the black-box. Note that OIP is a generalization of several oracle-computation problems where we need to determine all the $N = 2^n$ values of the truth table for a given oracle f_i. For example, the Grover search has an S of size N and each f_i in S is defined as $f_i(j) = 1$ iff $i = j$. The STACS paper proves among others that the query complexity of OIP is $O(\sqrt{N})$ for *any* S if $|S| = N$, which includes the upper-bound for the Grover search as a special case. Our main results in the current paper include: (i) The above algorithm for OIP with any S of size N can be made robust with a sacrifice of only a constant factor, i.e., its query complexity is still $O(\sqrt{N})$. To do this, we need to bypass the classical (noise-free) search which plays an important role in the original algorithm. (ii) A similar extension is also possible for the case that $|S| > N$. (Note that $|S|$ can be as large as 2^N.) In this case, our new algorithm is

not only robust but its query complexity is significantly better than the previous one.

4. S. Tani, M. Nakanishi, S. Yamashita:
"Quantum Protocol for the List-nonequality Function", Workshop on Quantum Information Processing 2005, Poster Presentation.
概要: In this paper, we show that a quantum protocol can do much better than classical protocols for a special case of the direct product problem, where we focus on computing the OR of the values of l instances of $2k$ input bit function f, i.e.,$f^{\vee l} = \bigvee_{i=1}^{l} f(x^i, y^i)$. In particular, we show an efficient quantum protocol to compute the list-nonequality function $LNE(l,k)$: the negation of $\mathrm{EQ}_k^{\vee l}$ where EQ_k means the equality function of k bits. It should be noted that the recursive calls of amplitude amplification technique used in the protocol for DISJ_n by Høyer et al. gives us a quantum protocol with $O(c^{\log^* l}\sqrt{l}\log k)$ communication bits. However, this is not necessarily better than the classical bound, i.e., $\Theta(l+\log k)$. To get a better bound than the classical one, we develop a quantum version of the classical public-private coin conversion: if there is a bounded error quantum protocol that uses classical public coins, a bounded error quantum protocol that does not use classical coins exists. By carefully combining this conversion with a robust quantum search by Høyer et al., we can show a quantum protocol whose complexity is $O(\sqrt{l}\log l + \log k)$.

研究会等

1. 河内亮周, 山下茂, 岩間一雄:
"オラクル同定問題に対する頑健な量子アルゴリズム", 情報処理学会研究会報告 アルゴリズム研究会, Vol. 96-1, pp. 1–8, 2004 年 7 月.
概要: オラクル同定問題とは n ビット入力 1 ビット出力のオラクルの集合 $S = \{f_1, ..., f_M\}$ と S に属する未知のオラクル f_i が与えられたとき，未知のオラクル f_i を S の中から同定する問題であり，数多くの問題の一般化になっている．本稿では，与えられた未知のオラクルクエリーの結果が正しい値と誤った値が重ね合わせ状態として出力される場合のオラクル同定問題（但し，誤った計算結果が得られる確率は 1/2 より小さい定数確率，例えば 1/10 以下とする.）に対して以下を示す．(i) 与えられたオラクル集合のサイズが $N = 2^n$ の場合（すなわち $M = N$.），エラー付きオラクル同定問題をクエリー回数 $O(\sqrt{N})$ で少なくとも定数確率で解く量子アルゴリズムが構成できる．(ii) 与えられたオラクル集合のサイズが N の場合，各 $x \in \{0,1\}^n$ で $f_i(x) = 1$ を満たす i の数に関するパラメータ K に関してある条件を満たすとき，エラー付きオラクル同定問題をクエリー回数 $O(\sqrt{N/K})$ で少なくとも定数確率で解く量子アルゴリズムが構成できる．

2. 谷誠一郎, 中西正樹, 山下茂:
"リスト型非等価関数を計算する量子プロトコル", 電子情報通信学会 量子情報技術研究会, QIT2004-51, pp. 21–25, 2004 年 12 月.
概要: This paper considers the quantum communication complexity of the list-nonequality function $LNE(l,k)$, which is AND of the values of l instances of the $2k$-bit nonequality function, i.e., the negation of OR of the values of l instances of the $2k$-bit equality function. We give the quantum communication complexity of $LNE(l,k)$ is at most $O(\sqrt{l}\log l + \log k)$ in the bounded error setting, which is asymptotically better than the corresponding classical complexity, i.e., $\Theta(l+\log k)$.

A08: 動的な構造をもつネットワーク上の資源割当て問題の研究

藤田 聡

広島大学 大学院 工学研究科
〒 739-8527 東広島市鏡山 1-4-1
fujita@se.hiroshima-u.ac.jp

1 はじめに

本研究課題の目的は、動的な構造をもつ大規模ネットワーク上の資源割当て問題の数理的な構造を明らかにし、その根本的な解決のための道筋を示すことである。本研究の柱は以下の 3 つである：

1) 動的ネットワーク上の資源割当て問題のモデル化と特徴づけ

2) 実時間性を考慮した新たな評価基準の考案とその妥当性の検証

3) 考案した評価基準のもとで最適なアルゴリズムの提案とその有効性の評価

研究初年度である平成 16 年度の目標は、その中でも 1) と 2) に焦点をあて、来年度以降の研究の具体的な方向性を定めることであった。

そのような目標にそって研究を進めた結果、本年度は以下のような成果をあげることができた。

a) サーバの位置が動的に変化する分散システムのための新しいモデル上で、ユーザへのサービスがサーバの移動に伴って中断しないようにするための、サーバ数に関する必要十分条件を明らかにした (2 節)。

b) 空間内にばらまかれたセンサーノードに対してその正確な位置情報を自律分散的に推定させる問題を考え、具体的なアルゴリズムを提案するとともに、その性能を実機を用いて実証した (3 節)。

c) システム内に存在する複数のユニットがお互いに故障診断をし合うようなモデルを考え、ハイパーキューブ状に接続されたユニット上では、3 ラウンドでの診断が必要かつ十分であることをはじめて証明した (4 節)。

d) 実時間性を考慮した新たな評価基準を探求するための手がかりとして、ネットワーク上の輻輳制御問題と加入制御問題について注目し、既知の手法の性能を実験的に評価するとともに、それらの問題点について詳細な検討を行った。

以下では、上記の a)〜c) について、背景と研究の位置づけを含めて、本研究課題の成果として得られた結果の概要を述べる。

2 移動サーバ割り当て問題

2.1 背景

近年、セルラーフォンシステムや無線 LAN など様々なネットワーク環境下で、高品質のサービスを安定して提供することが求められている。このようなサービスの多くでは、ノードの物理的な位置やオペレーティングシステムなどに関して透過 (transparent) であることが求められており、同一のサービスが “いつでもどこでも” 受けられることが強く要請されている。このことは、与えられたコンピュータネットワーク上に特定のサービスを提供するサーバをどのように配置すればよいかという問題を提起する。具体的には、ネットワーク上のどのノード上でサーバを立ち上げれば、コンテンツ配送のための遅延や、配送のためのパスのバンド幅、あるいは各サーバからサービスを受けるクライアント数の均等化などの意味で「良い」サーバの配置が実現されるかが重要な問題となる。またそのようなメトリックの多くは、物理的な距離の近さやバンド幅制約等を満足するノード間を論理的なリンクで結んで得られるオーバレイネットワークを考え、その上で支配集合 (dominating

set) となるようなノード集合上にサーバを配置することによって自然に実現することができる。

頂点集合 V と辺集合 E をもつネットワーク $G = (V, E)$ が与えられたとき、G の**支配集合** U とは、任意の頂点 $u \in V$ に対して、$u \in U$ であるか $\{u, v\} \in E$ かつ $v \in U$ であるような頂点 v が存在するような V の部分集合として定義される。グラフの支配集合はこれまでに多くの研究者によって精力的に研究されており、グラフ理論的な特徴づけや、最小サイズの支配集合を求めるための計算複雑度に関する研究、さらには区間グラフやパーフェクトグラフなど特別なクラスのグラフに対する多項式時間アルゴリズムの提案など、これまでに様々な結果が得られている。また支配集合の概念がネットワーク上のサーバ配置問題と関連していることも古くから指摘されており、最近では、アドホックネットワークのための効率的なルーティングに (連結) 支配集合をバックボーンとして利用しようという提案もなされている。

2.2 提案モデル

本研究では、支配集合の考え方に基づいた新しいサービス提供方式のモデルとして、あるホスト上に置かれたサーバが、サービス提供中にほかのホスト上に移動できるようなモデルを考える。そのようなサーバ機能の物理的な移動は、移動エージェントやプロセスマイグレーションの技術を用いることで実現することができるが、その際に問題となるのは、サーバの移動によってユーザに対するサービスが途切れないようにしなくてはならないという点である。すなわち、移動中を含む任意の時刻において、サーバの置かれた頂点集合が与えられたネットワークの支配集合となっていることが求められる (技術的な理由から、ここではリンク上を移動しているサーバはその両端点を同時に支配しているものとし、支配集合は多重集合であってもよいものと仮定する)。

以下では、2 つの支配集合 U_1, U_2 $(\subset V)$ が以下の条件を満たしているとき、支配集合間の関係の意味で隣接していると呼ぶことにする：

> 支配集合 U_1 中のある頂点 u を取り除き、$\{u, v\} \in E$ であるような頂点 v を加えることで、支配集合 U_2 が得られるとき。

また、支配集合間の隣接関係を推移的に適用して得られる関係を支配集合間の到達可能性と呼び、支配集合の集合 $\mathcal{D}$ $(\subset 2^V)$ に属している任意の 2 つの支配集合が支配集合のみを経由して互いに到達可能であるとき、集合 $\mathcal{D}$ は相互変換可能であると呼ぶ (ただし経由する支配集合は、$\mathcal{D}$ の要素である必要はない)。

本研究では、どのような条件を満たせば支配集合の集合が相互変換可能になるのかについて詳細に検討を行った。特に、ここでは対象となるグラフのクラスを木とハミルトングラフに限定し、支配集合の集合が相互変換可能になるためには支配集合のサイズがどのくらい大きくなくてはならないか、あるいはどのくらい小さくても大丈夫なのかについてあきらかにした。具体的には、以下の定理が成立する：

定理 1： n 個の頂点をもつ任意の木 T に対して、$k \geq \lfloor n/2 \rfloor$ 個の頂点からなるような T の支配集合たちは、相互変換可能である。また、任意の n に対して、最小支配集合のサイズが $\lfloor n/2 \rfloor$ であるような木 T が存在する。

定理 2： 任意の $r \geq 2$ と $n \geq 1$ に対して、サイズ $\lceil (n+1)/3 \rceil - 1$ の支配集合全体からなる集合 $\mathcal{D}$ が相互変換可能ではないような n 頂点のハミルトン r-正則グラフ G が存在する。

定理 3： n 頂点をもつ任意のハミルトングラフ G について、$k \geq \lceil (n+1)/3 \rceil$ 個の頂点からなるような G の支配集合たちは、相互変換可能である。

2.3 証明のスケッチ

以下では、それぞれの定理の証明のアイデアを簡単に説明する。

(定理 1 の証明のスケッチ) 葉 u を含むような支配集合が、u の代わりにその親頂点 v を含むような支配集合と (支配集合間の関係の意味で) 隣接している、という事実を利用する。頂点 v を支配集合に含めることで、少なくとも u, v の 2 頂点は (v によって) 支配されたことになるから、これらを木から取り除いて残りの部分に対して相互変換可能性を議論しても一般性を失わない。いま与えられた木に対する支配集合のサイズを $k \geq \lfloor n/2 \rfloor$ 個と仮定しているから、同様の議論を繰り返すこと

で、木に対する自明な支配集合に帰着させることができる。このことにより、定理の前半が証明できたことになる。後半部分については、中心となる根頂点がそれぞれの葉と長さ 2 のパスで結ばれているような木を考えればよい。葉の数は $\lfloor n/2 \rfloor$ 個あり、そのそれぞれが異なる頂点によって支配される必要があるため、このような木の最小支配集合のサイズは $\lfloor n/2 \rfloor$ となる。

(定理 2 の証明のスケッチ) $r = 1$ の場合は、サイズ $3m$ のリング (ただし m は整数) を考えればよい。サイズ $3m$ のリング上のサイズ $\lceil (n+1)/3 \rceil - 1 = m$ の支配集合は合計で 3 つ存在するが、それらの支配集合間を、支配集合のみを経由してお互いに行き来することはできない (サイズ m の支配集合に含まれる頂点のうちどれかひとつを隣接頂点に移動させると、支配集合ではなくなってしまう)。これは、サイズ m の支配集合に含まれる任意の頂点がそれぞれ 2 つの頂点を独占的に支配していることに起因する。定理 2 の証明では、この性質を利用したグラフの構成を行う。すなわち、サイズ m の支配集合に含まれる各頂点が、それぞれ 2 つの頂点を独占的に支配するような頂点数 $3m$ のグラフを具体的に構成することで、定理を証明することができる。

(定理 3 の証明のスケッチ) 証明は 2 つの部分から構成される。証明の前半部分では、支配集合のサイズが $\lceil (n+1)/3 \rceil$ 以上のとき、与えられたハミルトングラフ G とそのグラフに対する任意の支配集合 U から、G 上のハミルトン閉路 C の支配集合 U' に必ず到達させることができることを示す。後半部分では、サイズ n のリング上のサイズ $\lceil (n+1)/3 \rceil$ 以上の任意の 2 つの支配集合が、支配集合のみを経由してお互いに到達可能であることを示す。これらの 2 つの部分を組み合わせることにより、G 上のサイズ $\lceil (n+1)/3 \rceil$ 以上の任意の支配集合が、G 上のハミルトン閉路 C の支配集合を経由してお互いに到達可能であることを示すことができる。

証明の前半部分で使うキーテクニックは、具体的な相互変換を行う前に、U が支配集合であるような G の部分グラフを、辺を順次取り除くことであらかじめ求めておくことである。そのようにして得られた G の部分グラフは森となることが示せるから、木における支配集合に対する適切な操作を施すことで、(多少の場合分けは必要ではあるが、)C に含まれない辺を少なくとも 1 本以上取り除くことができるような支配集合への変換を実現することができる。

一方、後半部分では、リングサイズ n の 3 に関する剰余による場合分けを行うことで見通しよく議論を行うことができる。具体的には、まず最初に 3 による剰余が 2 である場合を考えると、これはサイズ $3m+2$ のリングがサイズ $m+1$ の支配集合によって支配されている状況に対応し、そのような任意の支配集合は、2 つの頂点によって支配されている唯一の頂点 u によって明確に特徴づけられることがわかる。u を支配している 2 つの頂点のうちどちらか一方を u から遠ざかる方向に移動させることで (隣接する) 新たな支配集合を得ることができ、そのような操作を繰り返し適用することで、任意の支配集合間の到達可能性を示すことができる (いまリングのサイズが 3 で割り切れない状況について考えていることに注意)。リングサイズ n の 3 による剰余が 1 である場合は、2 つの頂点によって支配されている頂点 u とその隣接頂点の合計 3 つの頂点をひとつの仮想的な頂点とみなし、剰余が 2 である場合と同様の議論を適用することができる。また剰余が 0 である場合は、さらにもう一段仮想的な頂点を考えればよい。

3 センサーノードへの位置情報配布問題

3.1 背景

ネットワーク上の資源配置のためのもうひとつの具体的な問題として、ユークリッド平面上に大量にばらまかれたセンサーノード (以下ノードと呼ぶ) たちに対して、各ノードの位置を無線通信機能を用いて正確に推定させる問題について研究を行った。この問題は一般に位置測位 (localization) 問題と呼ばれ、ユビキタスコンピューティングなどの分野で取り扱われる基本的な問題のひとつである。以下では、システム中には自身の正確な位置を知っている特別なデバイス (以下アンカーと呼ぶ) が複数存在し、ノードの位置測位は、アンカーたちとの通信を繰り返すことで実現されるものと仮定する。

本研究で対象とするのは、無線信号の送受信と、送受信装置間の距離変化による受信信号の強度変化の検出とができる程度の単純な構造をもったノードたちからなるセンサーネットワークであり、GPS (Global Positioning System) などで用いられている位相情報等に基づく距離推定機能は、チップサイズや消費電力などの制約から、ここでは仮定しない。提案する位置測位方式は、He らによって提案された PIT(Point-In-Triangle) テストに基づいている。PIT テストは、各アンカーとの距離を直接推定することなく各ノードの位置を測定することのできるいわゆるレンジフリー型の位置測位方式のための基本方式のひとつであり、信号を観測しているノードが 3 つのアンカーによって構成される三角形の内部に含まれているか否かを、以下の性質を利用して判定する：

> 観測点 M がアンカーによって構成される三角形 ABC の内部に存在するのは、M の近傍に、各アンカーから送られてくる信号の強度が同時に減少 (もしくは同時に増加) するような点が存在するときかつそのときに限られる。

PIT テストに基づく従来の位置測位方式 (APIT アルゴリズム) では、ノードの位置を微小変化させて信号強度の変化を見るのではなく、各ノードの周囲にすでに配置されているノードたちそれぞれの固定された位置における観測によって、ノード位置の変化を代替させるというアプローチがとられていた。しかしこのような方式では、観測位置の微小変化をほぼ同時刻に実現するためにはアンカーからの信号送信時刻を同期させるなどの付加機構が必要となり困難を伴うことから、送信時刻にばらつきが出てしまうことが予想され、そのことによって、観測結果が信号強度の時間変化の影響を直に受けてしまうという欠点がある。

3.2 提案モデル

提案手法では、観測位置の微小変化をノード側で実現するのではなく、アンカーの側で実現させる方法を新たに採用した。すなわち、複数のアンカーを少しずつ位置をずらして配置し、その位置関係と方角とを固定したまま空間内を移動できるようにして構成されたアンカーグループ (AG) という概念を導入し、PIT テストを行うための複数の三角形を、AG に空間内を時間をかけて移動させることによって実現することにした (もちろん同様の機能をもった AG を複数用意すれば、ノードの位置測位に要する時間は AG 数が増えた分だけ減少する可能性がある)。このことにより、測定位置の微小変化を AG に含まれるアンカーたちの同時送信によってほぼ同時刻にシミュレートすることが可能となり、PIT テストの精度を大幅に向上させることができる。この提案手法は、今年度、クラス 2 規格の Bluetooth デバイスを用いて実装され、いくつかの実証実験の結果、各観測点の位置測位が従来手法に比べて高精度に行えることが確かめられた。

またこの実装システムの成功をうけて、現在このモデル上で、以下のような理論的な問題について取り組んでいる：

- 位置測位に求められる分解能と移動時間や信号送信回数、AG の数などのコストが制約として与えられたとき、AG の移動スケジュールをどのようにすればよいか。
- 送信ポイントの数が与えられたとき、分解能をできるだけ向上させるような AG のスケジュールはどのようなものか。

スケジューラによって空間内に設定される送信ポイント間を線分で結ぶことによって、与えられた空間をいくつかの部分領域に分割することができるが、送信ポイント数を n としたとき、そのようにして得られる部分領域数の上限は $O(n^6)$ となることが知られている。この事実を利用することで、与えられたポイント数 n に対する分解能の下限を算出することができるが、最悪分解能という尺度で評価した場合、実際に得られる領域数は、それよりもはるかに少なくなる。具体的には、空間全体に関する最悪分解能は、送信ポイント集合から得られる凸包 (convex hull) 上の最長辺の長さよりも下回ることはない (その辺に内側から張り付いている部分領域の直径は辺の長さとほぼ等しくなる)。したがって今後は、AG の移動可能な領域と位置測位の対象となるノードの置かれている領域とを別々に分けて議論するなどの、さらに踏み込んだ議論が必要になると考えられる。

4　故障診断問題

4.1　背景

システムレベルの故障診断は、ディペンダブルな並列処理システムを実現する上で重要な課題のひとつである。システムレベルの故障診断という概念は、Preparata, Metze, Chien の 3 名によって 1967 年に提案され、その後様々な研究者によって研究が進められている重要な分野のひとつである。Preparata らによって提案されたモデル (PMC モデル) では、計算をおこなうユニット (コンピュータ) の集まりによって定義される並列処理システムを対象とし、各ユニットにはほかのユニットが正常に動作しているかどうかをテストする機能が与えられる。各ユニットによって行われたテストの結果はサーバ上に集められ、収集されたテスト結果は、故障診断アルゴリズムを用いて分析される。故障診断アルゴリズムの目的は、入力されたテスト結果の集まりから、故障しているユニット集合を正確に出力することである。PMC モデルのキーポイントは、正常なユニットによるテスト結果は常に正しいが、故障したユニットによるテスト結果は信頼できない、という点である。すなわち、疑わしいユニットをできるだけ減らし、正常であると確信できるユニットをできるだけ増やしていくことが、効率良く故障診断を行う上での基本的な方針となる。

オリジナルの PMC モデルでは、テストフェーズはちょうど 1 回だけ実行されていた。したがって故障診断のおもな目的は、与えられたテスト結果と矛盾しない最小個数の故障ユニットたちを正確に特定することであった (故障ユニット集合の最小性は、“すべてのユニットが故障している” などといった自明なケースを除外するために必要である)。故障ユニットの数が t を越えないという前提のもとで、すべての故障ユニットを正確に特定できるようなテストの集まりが存在するとき、そのシステムは t-診断可能であるという。t-診断可能なシステムは、少なくとも $2t+1$ 個のユニットをもたなくてはならず、その中の各ユニットがほかのユニットから少なくとも t 回は診断されなくてはならないことが知られている。したがって、ユニットの総数が N のとき、そのシステムが t-診断可能であるためには、少なくとも Nt 個のテストを実行する必要がある。t-診断可能システムのより一般的な特徴づけが Hakimi と Amin によってなされている。

4.2　研究の位置付け

1981 年に Nakajima は、故障診断の効率の向上を目的として、適応的な故障診断モデルを提案した。適応的な故障診断は (通常の故障診断とは異なり) 複数のテストラウンドから構成され、テスト数を少なくすると同時に、テストのためのラウンド数を少なくすることが、適応的な故障診断問題のおもな目的となる。与えられたネットワークが完全結合しているとき、t 個の故障ユニットを正しく特定するのに必要十分なテスト数は、適応的な故障診断モデルを適用することで、通常のモデルの Nt 個から $N+t-1$ 個に大幅に減少することが知られている。また各ユニットが 1 回のラウンドで複数のテストに参加することを禁止するようなモデルのもとでも、与えられたネットワークが完全グラフであれば、すべての故障ユニットを正しく特定するために必要なラウンド数が定数で抑えられることもわかっている。

適応的な故障診断モデルの診断能力は、木、サイクル、トーラス、バタフライネットワーク、キューブ・コネクテッド・サイクル (CCC) など、いくつかのグラフのクラスについても詳細に調べられている。それらの中でも、Feng らによって示されたバイナリハイパーキューブに関する結果は、注目に値する。Feng らは、n 次元バイナリハイパーキューブ (以下 n-キューブ) 上で高々n 個の故障ユニットしか存在しないとき、高々$(n+4)$ 回のラウンドと高々$2^n(\lceil \log n \rceil + 2)$ 個のテストですべての故障ユニットを正しく特定できることを証明した (n-キューブは n 個の完全マッチングに因子分解できるから、自明なラウンド数とテスト数の上界は、それぞれ $2n$、$n2^{n+1}$ であることに注意)。この結果はのちに Kranakis と Pelc によって 11 ラウンドと $2^n + 3n/2$ テストに改良され、これはさらに Björklund によって 4 ラウンドにまで改良された。(Björklund はラウンド数の改良に加え、n-キューブ上の適応的な故障診断では $2^n + n - 1$ 個のテストが必要十分であることも示している)。またこれと同じ論文で、Björklund は

ラウンド数の下界が 3 であることも示している。ごく最近、Nomura らによって、故障ユニット数が高々$n - \lceil \log(n - \lceil \log \log n \rceil + 4) \rceil + 2$ であれば、3 回のラウンドが必要十分であることが示されたが、一般の場合に何ラウンドが必要十分であるかについては、これまで未解決であった。

4.3 基本アイデア

本研究では、任意の $n \geq 3$ に対して、故障ユニット数が n を越えない限り、n-キューブ上の適応的な故障診断が 3 ラウンドで行えることを示した。この結果は、以下の 3 つの意味で最適である：1) Björklund の結果から適応的な故障診断には少なくとも 3 ラウンドが必要であること、2) n-キューブ上には、どのような故障診断方式によっても特定不可能な $n+1$ 個の故障ユニットの配置が存在すること、3) n-キューブ上上で n 個の故障ユニットを特定するためには、システムは少なくとも $2n+1$ 個のユニットをもたなくてはならないこと (すなわち $n = 3$ というのは、$2^n \geq 2n+1$ を満たすもっとも小さい整数である)。

提案する故障診断アルゴリズムの概要は、以下の通りである：まず一般性を失うことなく $n \geq 3$ とし、m を $m = \lceil \log_2(n+1) \rceil$ を満たす整数とする。ここで $2^m \geq n+1$ であり、しかも任意の $n \geq 3$ について $m < n$ であることに注意しよう。構成法の最初のステップとして、与えられた n-キューブを 2^{n-m} 個の m-キューブ、$P_1, P_2, \ldots, P_{2^{n-m}}$、に分割する。ここで各 m-キューブは、長さ $n-m$ の同一のプレフィックスをもつような頂点たちから構成されるものとする。構成された m-キューブたちに対して、グレイコードに基づくハミルトンサイクルをそれぞれ構成する。適応的故障診断の最初の 2 ラウンドでは、そのようにして構成された 2^{n-m} 個のハミルトンサイクルに沿って、それぞれ独立に故障診断を行う。各 m-キューブの頂点数が $n+1$ 以上であり、システム全体の故障数が n 以下であることを仮定しているから、もし最初の 2 ラウンドで異常が報告されなければ、その m-キューブには故障ユニットは含まれないことになる。換言すれば、異常を示すテスト結果を含む m-キューブは高々 n 個しか存在しないはずである。そのような m-キューブの個数を x とおき、最初の 2 ラウンドの結果、故障ユニットを含むと判断された m-キューブの集合を $\mathcal{Q} = \{P_1, P_2, \ldots, P_x\}$ とおくことにする。

もし $x \leq n-m$ ならば、以下のようにもう 1 ラウンドだけ費やすことで、故障ユニットの特定を簡単に行うことができる：先に求めた 2^{n-m} 個の m-キューブのそれぞれを仮想的な頂点とみなし、隣接する頂点を内部に含む仮想的な頂点どうしをリンクで結んで得られる $(n-m)$-キューブを考え、これを $\hat{Q}_{n-m}$ と記すことにする。また、$\mathcal{Q}$ の各要素に対応する $V(\hat{Q}_{n-m})$ 中の x 個の仮想的な頂点の集合を U とおく。いま $x \leq n-m$ であるから、Hull の定理を用いることで、$\hat{Q}_{n-m}$ の中に以下のような性質をもつ仮想頂点の集合 $W \subset V(\hat{Q}_{n-m}) - U$ が存在することを示すことができる：W と U の間に ($\hat{Q}_{n-m}$ に関する) 完全マッチングが存在すること。いま U 以外の仮想頂点は故障ユニットを含まないことが仮定と最初の 2 ラウンドの結果から保証されているため、U と W を結ぶリンク集合を使って診断を行えば、U 中のどのユニットが故障しているかを正しく特定することが可能となる。

一方 $n-m+1 \leq x \leq n$ の場合は、以下のようにして故障診断を行うことができる。$\mathcal{Q}$ に含まれる各 m-キューブは、少なくとも 1 個の、そして高々 m 個の故障ユニットを含んでいる (もし $m+1$ 個以上の故障ユニットを含む m-キューブが存在すれば、故障ユニット数は少なくとも $m+1+(x-1) \geq n+1$ 個となり、仮定に矛盾してしまう)。このことは、故障の存在を示すそれぞれのテスト結果に対して、長さ m のパス上のユニットの故障のみをチェックすればよいということを意味している (最初の 2 ラウンドのテスト結果はサイクル状になっているから、そのうちの長さ m の部分だけを取り出してチェックすればよい)。そのようなチェックを 1 ラウンドで実現するため、ここでは “どれだけの長さのパスについてチェックすればよいか” をあらわすパラメータ m' を導入し、この値を再帰的に小さくしていくことでどのような故障のパターンに対しても正しく判定が行えることを示している。パラメータ m' は m に初期化され、再帰を一回行うごとに (すなわちそれまでの深さでは特定できないと判断された場合に)、対数関数的に減少していく。

研究業績一覧

学術論文

1. H. Osada, S. Fujita:
   "CHQ: A Multi-Agent Reinforcement Learning Scheme for Partially Observable Markov Decision Processes", IEICE Trans. Inf. & Syst., （掲載予定）.
   概要: In this paper, we propose a new reinforcement learning scheme called CHQ that could efficiently acquire appropriate policies under partially observable Markov decision processes (POMDP) involving probabilistic state transitions, which frequently occurs in multi-agent systems in which each agent independently takes a probabilistic action based on a partial observation of the underlying environment. A key idea of CHQ is to extend the HQ-learning proposed by Wiering *et al.* in such a way that it could learn the activation order of the MDP subtasks as well as an appropriate policy under each MDP subtask. The goodness of the proposed scheme is experimentally evaluated. The result of experiments implies that it can acquire a deterministic policy with a sufficiently high success rate, even if the given task is POMDP with probabilistic state transitions.

2. D. Takemoto, S. Tagashira, S. Fujita:
   "Distributed Zone Partitioning Schemes for CAN and its Application to the Load Balancing in Pure P2P Systems", 情報処理学会論文誌, 46(2), 348–356, （Feb. 2005）.
   概要: In this paper, we propose several distributed zone partitioning schemes for Content-Addressable Networks (CAN), which is known as a pure peer-to-peer system based on the Distributed Hash Table (DHT). The main objective of the proposed schemes is to balance the load of nodes in the CAN system, in such a way that every node receives almost the same number of inquiries from the other nodes in the system. The result of simulations implies that, by using the proposed schemes instead of a randomized scheme originally implemented in the CAN system, we could reduce the response time for each inquiry to less than 75%.

3. M. Mito, S. Fujita:
   "On Heuristics for Solving Winner Determination Problem in Combinatorial Auctions", Journal of Heuristics, 10, 507–523, (2004).
   概要: The winner determination problem (WDP) in combinatorial auctions is the problem of, given a finite set of combinatorial bids $\mathcal{B}$, finding a feasible subset $\mathcal{B}'$ of $\mathcal{B}$ with a maximum revenue. WDP is known to be equivalent to the maximum weight set packing problem, and hard to approximate by polynomial time algorithms. This paper proposes three heuristic bid ordering schemes for solving WDP; the first two schemes take into account the number of goods shared by conflicting bids, and the third one is based on a recursive application of such local heuristic functions. We conducted several experiments to evaluate the goodness of the proposed schemes. The result of experiments implies that the first two schemes are particularly effective to improve the performance of the resulting heuristic search procedures. More concretely, they are scalable compared with the conventional linear programming (LP) relaxation based schemes, and could quickly provide an optimum solution under optimization schemes such as the branch-and-bound method. In addition, they exhibit a good anytime performance competitive to the LP-based schemes, although it is sensitive to configurable parameters controlling the strength of contributions of bid conflicts to the resultant bid ordering schemes.

4. 田頭, 吉岡, 藤田:
“周辺情報検索におけるプロキシシステムのためのキャッシュ置換アルゴリズム”, 情報処理学会論文誌, 45(10), 507–523, （2004）.
概要: 本論文では、クライアント・サーバモデルを用いた周辺情報検索システムにおいて、プロキシ型のキャッシュシステムを導入することを考え、そのプロキシキャッシュ上での効果的なキャッシュ置換アルゴリズム (LFU-FF 法) を提案する。LFU-FF 法は、参照の局所性に加えて周辺情報のデータ構造を考慮して、周辺情報に適したキャッシュデータの置き換えを実現する。具体的には、本研究で対象とするシステムでは、周辺情報のデータ構造において地理的な隣接関係を記憶領域上での連続関係として保持することにより、検索エリアに該当する周辺情報への高速な連続アクセスを実現している。LFU-FF 法では、この構造を利用してキャッシュ内での周辺情報の連続性と参照回数を評価値として用い、キャッシュデータの追加または削除を行う。LFU-FF 法を採用したプロキシシステムのプロトタイプシステムを構築し評価を行った、結果として、LFU 法と比べて、キャッシュサイズが全体の 8 %のときに、応答時間を約 21 %向上することができた。

5. H. Ochi, S. Tagashira, S. Fujita:
“A Localization Scheme for Sensor Networks Based on Wireless Communication with Anchor Groups”, Proc. The 11th International Conference on Parallel and Distributed Systems (ICPADS 2005), （掲載予定）.
概要: In this paper, we propose a new localization scheme for wireless sensor networks consisting of a huge number of sensor nodes equipped with simple wireless communication devices such as wireless LAN and Bluetooth. The proposed scheme is based on the Point-In-Triangle (PIT) test proposed by He *et al.* The scheme is actually implemented by using Bluetooth devices of Class 2, and the performance of the scheme is evaluated in an actual environment. The result of experiments indicates that the proposed scheme could realize a localization with an error of less than 2 m.

6. S. Fujita, S. Tagashira, C. Qiao, M. Mito:
“Distributed Branch-and-Bound Scheme for Solving the Winner Determination Problem in Combinatorial Auctions”, Proc. the IEEE 19th International Conference on Advanced Information Networking and Applications (AINA 2005), （掲載予定）.
概要: In this paper, we propose a new class of parallel branch-and-bound (B&B) schemes. The main idea of the scheme is to focus on the *functional parallelism* instead of conventional *data parallelism*, and to support such a heterogeneous and irregular parallelism by using a collection of autonomous agents distributed over the network. After examining several design issues toward the implementation of a prototype of the distributed B&B system, we illustrate the result of our preliminary experiments conducted to estimate the performance of the proposed scheme. The result shows that it could cause a significant performance improvement if each agent autonomously changes its function type according to the change of the underlying environment.

7. S. Fujita:
“A Note on Efficient Key Location in Pure P2P Systems under an Environment with Dynamic Key Modifications”, Proc. the IASTED International Conference on Parallel and Distributed Computing and Networks (PDCN 2005), CD-ROM, (Feb. 2005).
概要: In this paper, we consider the problem of finding a key from elements distributed over a peer-to-peer (P2P) system, where elements locally stored in each node are drawn from a totally ordered set such as the set of integers and the set of English

words. As the basic technique to realize an efficient key location, we focus on the combination of binary search and an approximated sorting of the elements. We provide a detailed analysis of the sorting-based key location scheme, and indicate possible directions for further research.

8. S. Fujita, T. Araki:
"Three-Round Adaptive Diagnosis in Binary n-Cubes", Algorithms and Computation, 15th International Symposium, ISAAC 2004, Hong Kong, China, December 2004, Proceedings (R. Fleischer, G. Trippen Eds.), LNCS 3341, 442–451, (2004).
概要: In this paper, we consider the problem of adaptive fault-diagnosis in binary n-cubes, and propose a scheme that completes a diagnosis in at most three test rounds, provided that $n \geq 3$ and the number of faulty vertices is at most n. The proposed scheme is optimal in the sense that: 1) three rounds are necessary for the adaptive diagnosis, 2) there exists a set of $n + 1$ faulty vertices that can not be located by any diagnosis scheme, and 3) to identify n faulty vertices, the system must contain at least $2n + 1$ vertices. Note that $n = 3$ is the smallest integer satisfying $2^n \geq 2n + 1$.

9. S. Fujita, Y. Liang:
"How to Provide Continuous Services by Mobile Servers in Communication Networks", Parallel and Distributed Computing: Applications and Technologies, 5th International Conference, PDCAT 2004, Singapore, December 2004, Proceedings (K.-M. Liew, H. Shen, S. See, W. Cai, P. Fan, S. Horiguchi, Eds.), LNCS 3320, 326–329, (2004).
概要: In this paper, we propose a new framework to provide continuous services by "mobile servers" in interconnection networks. In particular, we prove that for the classes of ring networks with n vertices, $\lceil (n+1)/3 \rceil$ mobile servers are necessary and sufficient to realize mutual transfers among configurations dominating the network, where transfer between two dominating configurations is realized by moving the role of dominating vertex from a vertex to an adjacent vertex.

10. A. Ohtsubo, D. Takemoto, S. Tagashira, S. Fujita:
"The Power of Shortcuts in Greedy Routing in Content Addressable Networks", Embedded and Ubiquitous Computing, International Conference, EUC 2004, Proceedings (L. T. Yang, M. Gua, G. R. Gao, N. K. Jha, Eds.), LNCS 3207, 994–1003, (2004).
概要: In this paper, we propose a scheme to dynamically establish shortcut links in Content Addressable Networks (CAN), based on a probabilistic method suggested by Kleinberg in 2000. The proposed scheme consists of the following three steps: 1) estimation of the total number of nodes participating to the P2P system, 2) dynamic adjustment of the probability distribution for selecting the target point of shortcut based on the estimated number, and 3) the establishment of shortcut to the nodes corresponding to the selected points. The performance of the resulting scheme is evaluated by simulation. The result of simulations implies that the shortcut significantly reduces the average number of hop counts, and the rate of improvement increases as increasing the number of nodes; e.g., the proposed method improves the hop counts in conventional CAN by 49% when it contains 4096 nodes. In addition, dynamic adjustment of the probability distribution improves the performance of the overall scheme, although the amount of improvement is less than "one hop" for relatively small netwotks examined in the simulation.

11. H. Kutsuna, S. Tagashira, S. Fujita:

"Experimental Evaluation of Bimodal Congestion Control Scheme in High-Speed Networks with Broad Bandwidth", Proc. the 2004 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS 2004), III-227–III-230, (2004).

概要: In this paper, we study congestion control schemes in high-speed networks. We focus on Bimodal congestion control scheme proposed by Attie *et al.*, as an alternative to AIMD that is used in the current TCP. By the result of extensive simulations, we found that although Bimodal could improve the throughput of AIMD by 10% in low-speed networks, the amount of improvements will be limited in high-speed networks because of the high frequency of retransmissions of packets.

12. M. Yamane, S. Tagashira, S. Fujita:
"Admission Control of Predictive Services under an Environment with Frequent Retransmissions of Packets", Proc. the 2004 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS 2004), II-681–II-684, (2004).

概要: In this paper, we consider the admission control of communication flows under an environment with frequent retransmissions of packets. The basic idea of the proposed scheme is to improve Jamin *et al.*'s predictive service so as to take into account the effect of retransmissions of packets in a parameterized manner. The goodness of the scheme is evaluated by simulation. The result of simulations indicates that the proposed scheme can guarantee a predetermined delay bound without degrading the link utilization rate by appropriately selecting the value of a configurable parameter.

研究会等

1. 中尾, 水戸, 田頭, 藤田:
"P2P オーバレイネットワークにおけるプローブを用いた共有情報の範囲検索法", グループウェアとネットワークサービスワークショップ 2004(GNWS2004), 69–74, (2004.11).

概要: P2P 環境では、様々な属性をもつ情報が多くの計算機 (ピア) により共有されている。これらの共有情報の中から、特定の属性に対して、ある範囲内に含まれる情報を発見する範囲検索技術が注目されている。このような検索を P2P 環境で実現するためには、頻繁に発生するピアの参加・離脱を想定した効率的な手法が必要である。本研究では、リング型のオーバレイネットワークをピア間で構築し、そのネットワーク上にショートカット (プローブ) を付加して P2P 環境に適した範囲検索手法を提案する。提案手法では、プローブを用いて効率的な検索を実現し、さらに、楽観的にプローブの付加と管理をおこなうことで、参加・離脱に伴うオーバレイネットワークの変化に柔軟に対応する。我々は提案手法を実験により評価し、その有効性を確認した。その結果から、提案手法は様々な属性値の分布に対して、平均 $O(\sqrt{n/d})$ ステップで目的とする情報を発見できることがわかった。

2. 梅實, 藤田:
"リンケージ同定を導入した TSP のための進化計算解法の提案", 電子情報通信学会 ニューロコンピューティング研究会, Vol.104, No.474, 49–54, (2004.11).

概要: 本稿では，遺伝的アルゴリズム (GA) のための新しいリンケージ同定法の提案と評価を行なう．GA は組合せ最適化問題のためのメタ解法のひとつとして注目されており，これまでにその改良や実装に関する数多くの提案がなされている．提案手法では，組合せ最適化問題のための GA 解法においては "遺伝子間の関係" が特に強い意味をもっていることに着目し，それらの関係を考慮した高精度のリンケージ同定を DSMGA 法を改良することで実現している．提案手法の性能は，TSP のためのベンチマークセットである TSBLIB を用いて実験的に評価された．その結果，提案手法には比較的精度の高い解を少

ないばらつきで生成する効果があることが明らかになった.

3. C. Qiao, M. Mito, S. Tagashira, S. Fujita: "Parallel Branch-and-Bound Scheme for the Winner Determination Problem in Combinatorial Auctions", 情報処理学会 計算機アーキテクチャ研究会, No.2004-ARC-160, 23–28, (2004.12).
概要: In this paper, we propose a new class of parallel branch-and-bound (B&B) schemes. The main idea of the scheme is to focus on the *functional parallelism* instead of conventional *data parallelism*, and to support such a heterogeneous and irregular parallelism by using a collection of autonomous agents distributed over the network. After examining several design issues toward the implementation of a prototype of the distributed B&B system, we illustrate the result of our preliminary experiments conducted to estimate the performance of the proposed scheme. The result shows that it could cause a significant performance improvement if each agent autonomously changes its function type according to the change of the underlying environment.

4. 越智, 田頭, 藤田: "無線センサーネットワークを利用した位置測位システムの構築", 情報処理学会 計算機アーキテクチャ研究会, No.2004-ARC-160, 17–22, (2004.12).
概要: ユビキタスコンピューティング環境における重要な課題のひとつに, 実空間におけるヒトやモノの位置情報を如何にして正確に把握するかという問題がある. 本稿では, 無線通信機能を搭載した微小なデバイスたちからなるセンサネットワークを対象とし, ある領域に分散された各センサノードが, 外部から与えられる情報をもとに, 自身の位置情報を自律的に獲得していくための新しい手法の提案と評価を行なう.

5. 小畠, 竹本, 田頭, 藤田: "P2P システム上でのリザルトキャッシングを用いた条件付検索手法", 電子情報通信学会 ネットワークシステム研究会, Vol.104, No.513, 7–12, (2004.12).
概要: P2P システム上で共有資源を効率的に管理するための手法のひとつとして, DHT(分散ハッシュテーブル) を用いた情報管理手法が注目されている. 本稿では, DHT を用いた P2P システム (P2P DHT) 上で AND 検索や OR 検索のような条件付き検索を効率的に実現するための手法の提案を行う. 提案手法では, 一度検索した結果を各ピアがローカルにキャッシュし, その情報を将来ほかのピアが行う検索で再利用することで, 検索コストの大幅な削減を図っている. また各ピアから出された検索内容をキャッシュ内に存在する情報とうまく関連付けることで, キャッシュの利用率を向上させる試みもあわせて行っている. 提案手法の有効性はシミュレーションにより評価される.

6. S. Fujita, Y. Liang: "On the mutual transferability among dominating sets in graphs", 情報処理学会 アルゴリズム研究会, 2005-AL-099, (2005.1).
概要: In this paper, we propose a new framework to provide continuous services by "mobile servers" in interconnection networks. We model those mobile servers as a subset of host nodes, and assume that a node can receive the service if at least one adjacent node plays the role of a server (i.e., we assume that the service could not be routed via the interconnection network). The main results are summarized as follows: For the classes of trees with n vertices, $\lceil (n+1)/2 \rceil$ mobile servers are necessary and sufficient to realize continuous services by the mobile servers, and for the classes of Hamiltonian graphs with n vertices, $\lceil (n+1)/3 \rceil$ mobile servers are necessary and sufficient.

7. T. Tao, S. Tagashira, S. Fujita: "Performance Evaluation of Q-routing Pro-

tocol for Mobile Ad-hoc Networks", 情報処理学会 システム評価研究会, (発表予定).

概要: In this paper, we propose a new routing protocol for mobile ad-hoc networks (MANET), that have attracted considerable attentions in recent years as a tool to realize flexible and robust communication environments in many critical application fields. The proposed protocol, called LQ-routing, is a proactive routing protocol based on the Q-routing proposed by Littman and Boyan in 1993. In order to reflect the mobility of hosts to the routing decision, that would cause frequent connection and disconnection of communication links between nearby hosts, we introduce the notion of lifetime to represent the stability of routes connecting to the destination. The performance of the proposed routing scheme is experimentally evaluated by using NS-2. The result of simulation implies that by introducing the notion of lifetime to a simple combination of previous proactive routing scheme DSDV and the Q-routing, we could improve the performance of DSDV in terms of the packet loss rate and the average packet delay.

A09: 非明示的表現に対するアルゴリズムの開発

篠原　歩 †　竹田　正幸 †　下薗真一 ‡　坂本　比呂志 ‡

† 九州大学 大学院 システム情報科学研究院
〒 812-8581 福岡市東区箱崎 6-10-1
{ayumi,takeda}@i.kyushu-u.ac.jp

‡ 九州工業大学 情報工学部 知能情報工学科
〒 820-8502 福岡県 飯塚市 大字川津 680-4
{sin,hiroshi}@ai.kyutech.ac.jp

1　研究の概要

本研究は，非明示的に表現されたオブジェクトに対するアルゴリズムの開発とその計算量の解析を行うことと，また同時に，効率のよいアルゴリズムの開発に適した非明示的な表現法を見つけ出すことを目的として，主に文字列やグラフなどの離散構造を対象として研究を展開している．

初年度にあたる本年度はまず，グラフの非明示的な表現として多くの応用例が知られている順序付き二分決定ダイアグラム (OBDD) に着目し，文字列を OBDD で表現する方法を考え，これを文法の形で定式化しなおした．こうして非明示的に表されたパターン文字列とテキスト文字列が与えられたときに，それを陽に展開せずにパターン照合を行うアルゴリズムを開発した．また，コラージュシステムと呼ばれる文法型式で与えられた文字列に関しても，その部分族に関して既存のものよりも高速に照合を行えるアルゴリズムを与えた．また文脈自由文法の部分クラスにおいても同様の解析を行った．逆に，与えられた文字列からそれを表す小さなサイズの文法を見つける問題はデータ圧縮の一種とみなせるが，我々は領域効率のよい線形時間の圧縮アルゴリズムを開発した．また，１次元または２次元に散らばった点の集合に対する近似的な照合を行うアルゴリズムも開発した．一方，文字列照合を行う非決定性の有限オートマトンの状態遷移をビットベクトルで表し，ビット演算によって高速な照合を行うビット並列の手法を用いて，日本語のような複数バイト文字列に対してもそのまま効率よく働くアルゴリズムの与えた．また，挿入と削除のみを許し，置換を許さない状況下での近似文字列照合に関して，既存のものよりも高速なビット並列アルゴリズムも示し，これらのアルゴリズムの有効性を計算機実験によって実証した．また，パターン集合を特徴づける文字列パターンを高速に発見するアルゴリズムとデータ構造の開発を行った．以下に，これらの研究成果についてより具体的に述べる．

2　データ圧縮とパターン照合

テキスト文字列の中から目的とするパターン文字列の出現を検出する文字列パターン照合問題は，情報検索における最も基本的な問題として古くから盛んに研究され，Knuth-Moriss-Pratt 法や Boyer-Moore 法をはじめとして多くの効率的なパターン照合アルゴリズムが提案されてきた．しかし，一般にテキストはディスクなどの二次記憶装置に格納されるため，処理時間の大半がテキストのデータ転送に費やされることになる．したがって，パターン照合アルゴリズム自体の改良によって処理時間を短縮することには限界ある．

そこで，テキストをあらかじめ圧縮しておくことによってデータの転送量を減らして高速化を測る方式も提案されてきた．その際，圧縮テキストを復号した上でパターン照合を行ったのでは復号する手間がかかり高速化の妨げとなるため，圧縮テキストを陽に復号せずにそのままパターン照合処理を行おうという，**圧縮パターン照合**の技法に注目が集まっている．すなわち，入力となるテキストが，文字列そのものではなく，他の構造であり，したがって，その入力長そのものの測り方が変わってくることになり，その様相は一変する．また場合によってはテキストのみならず，パターンも他の構造で圧縮表現されたものを考える場合もある．本研究では，以下に示すとおり，文字列や点列を対象とした圧縮パターン照合アルゴリズムや，圧縮アルゴリズムの高速化を行った．

2.1 文法を用いた文字列圧縮

データ圧縮法の性能は，圧縮率，圧縮/展開時間，および主記憶量で決まるが，一般にこれらはトレードオフの関係にあり，すべてを高水準に保つことは難しい．例えばBW変換を利用した圧縮法は圧縮率こそ良いものの，原理的に線形時間での圧縮は不可能である．また，算術符号化も圧縮率はよいものの，時間と主記憶の両方を大量に消費する．本研究では，文字列を一意に表す文法を用いて，これらのリソースの消費を最小限に抑えつつ，理論的な限界に近い圧縮率を達成する高速な圧縮アルゴリズムを考案し，実装した．ここで取り扱う文法による圧縮問題は，次のような最適化問題として定式化できる．

入力 文字列 $w \in \Sigma^*$

出力 $L(G) = \{w\}$ となる決定性の文脈自由文法 G.

評価尺度 文法 G の大きさ

この問題に対して，まず論文 [9] において，線形時間で動作する近似アルゴリズムを与えた．その近似率は，$O(\log \frac{n}{g_*})$ である．ここに $n = |w|$ であり，g_* は，$L(G) = \{w\}$ となる最小の決定性の文脈自由文法の大きさである．このときの領域使用量は $O(n)$ である．さらに，論文 [10] において，近似率は，$O(\log g_* \log n)$ とやや劣るものの，領域使用量を $O(g_* \log g_*)$ に抑えた線形時間の圧縮アルゴリズムを与えた．またこれを実データに対して適用し，その効果を実験的に評価した．

2.2 文法圧縮に対するパターン照合

さらに，以下のように定義される文法表現に対する圧縮文字列照合アルゴリズムを考案した．次のような変数代入の列によって表される文法表現 $\mathcal{T}$ を *MPM* とよぶ．

$$\begin{aligned} X_1 &= expr_1, \\ X_2 &= expr_2, \\ &\vdots \\ X_n &= expr_n \end{aligned}$$

ここにおのおのの X_i は変数であり，$expr_i$ は次のような形の式である：

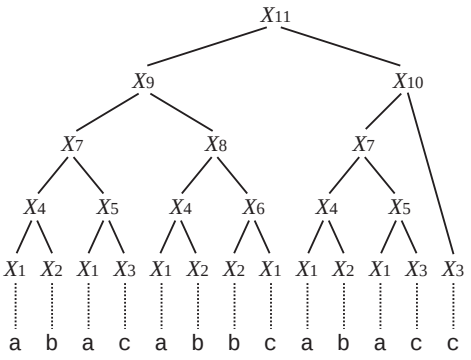


図 2.1: 文字列 abacabbcabacc に対する MPM の導出木.

- $expr_i = a$ $(a \in \Sigma)$, または
- $expr_i = X_\ell X_r$ $(\ell, r < i)$ ただし $|X_\ell| \geq |X_r|$ と $|X_\ell|$ は 2 のベキ数する．

MPM $\mathcal{T}$ は，$L(\mathcal{T}) = \{T\}$ となる，チョムスキー標準型の文脈自由文法の一種であるとみなすことができる．$\mathcal{T}$ のサイズは n であり，$\|\mathcal{T}\|$ と表す．例えば，文字列 $T =$ abacabbcabacc に対する MPM $\mathcal{T}$ は次のようになる．

$$\begin{aligned} X_1 &= \mathtt{a}, \\ X_2 &= \mathtt{b}, \\ X_3 &= \mathtt{c}, \\ X_4 &= X_1X_2, \\ X_5 &= X_1X_3, \\ X_6 &= X_2X_3, \\ X_7 &= X_4X_5, \\ X_8 &= X_4X_6, \\ X_9 &= X_7X_8, \\ X_{10} &= X_7X_3, \\ X_{11} &= X_9X_{10} \\ \\ \mathcal{T} &= X_{11}. \end{aligned}$$

この $\mathcal{T}$ に対する導出木を図. 2.1 に示す．

このとき，$\|\mathcal{T}\| = 11$ であり，その表す文字列 T の長さは 13 であることに注意されたい．一般に，$\mathcal{T}$ の表現長 $\|\mathcal{T}\|$ に対して，$\mathcal{T}$ が表す文字列 T の長さは指数的に長くなりうる．一方で，ここで考えている文法では，「$|X_\ell| \geq |X_r|$ と $|X_\ell|$ は

2 のベキ数する」という制約条件が付けられており，この制限によって構文木の形が大きく制限されることになる．

MPM に対するパターン照合問題とは，与えられた 2 つの MPM $\mathcal{T}$ と $\mathcal{P}$ に対し，それぞれを展開して得られる文字列 T と P をそれぞれテキストとパターンとみなして，T の中に P が現れる位置をすべて見つけ出す問題である．

上記の制約条件がない場合には，宮崎ら [8] による $O(m^2n^2)$ 時間 $O(mn)$ 領域のアルゴリズムが現在知られている中で最も高速な圧縮文字列照合アルゴリズムである．ここに $\|\mathcal{T}\| = n$ および $\|\mathcal{P}\| = m$ である．それに対し，我々は，この制約を巧みに利用することによって計算時間を $O(mn^2)$ 時間に短縮することができた [6].

2.3 点列の圧縮パターン照合

通常，我々が文字列について考察する場合，有限アルファベット上のものを対象とする．一方，点列（数値列）は，文字列のアルファベットを無限に拡張したものとみなすことができる．しかしながら，その点列の表現長は，実際に点列が空間を占める長さに対して log オーダーとなりうるため，ランレングス・コーディングと同様な圧縮された表現ととらえることができる．そのため，パターン照合を行う際には通常の文字列検索とは異なる様相を呈する．我々は，論文 [12] において，その違いを克服して文字列の近似照合と同じオーダーで動作する点列のための近似照合アルゴリズムについて，現実的な解法を与えるという観点から議論した．また逆に，文字列に対する照合アルゴリズムの高速化として用いられるテクニックを適用するための条件と，応用方法についても議論した．

線形変換による**点列パタン照合問題**は, ユークリッド空間上の 2 つの点集合パタン P とテキスト T が与えられた時, P を T の部分集合に写像する線形変換を見つける問題である. 本研究ではまず, 主軸について昇順の 1 次元の点列に対して, 平行移動と点の間の空間の挿入 · 削除による編集距離とそれに基づく近似点列パタン照合問題を定義した．次に P のサイズ n, T のサイズ m について時間計算量 $O(nm^2)$ で動作する近似点列パタン照合問題のアルゴリズムを紹介し, 高速化のための改良を加えたアルゴリズムが有限解像度を持つ P, T に対して $O(nm)$ で動作することを証明した．更に「4 人のロシア人の方法」として知られている手法を応用して $O(\frac{nm}{\log m} + m\log^2 m)$ 時間に高速化する技法を示した．そして, 多項式時間で解くことができる 2 次元近似点列パタン照合を提案した．これらの方法は，2 次元の点列の 1 次元目の値を音の発音のタイミングとし，また 2 次元目の値を音高とすれば，音楽データに対する近似照合問題の定式化のひとつとみなすことができ，この方面への応用も見込まれる．

2.4 XML データの圧縮パターン照合

XML データを圧縮する試みは 2000 年頃から行われているが，初期の頃に提案された XMill や xmlppm などは，圧縮のみに焦点を置いた研究であり，データ検索を行うことはできなかった．その後，圧縮データを展開しながら検索を行うことができる XGrind などが提案されたが，データを展開することがボトルネックとなっており，データを大規模化することができなかった．こうした背景の中で，データを圧縮したまま検索するための手法として，XPress が提案された．この手法は高速ではあるが，いくつかの欠点を持っている．まず，この手法は算術符号化のある性質に依存しているため，ごく限定された形式の検索しかできない．また，元データの構造を一部破棄してしまうため，データの追加/削除が難しく，特に，データの部分的な更新は不可能である．このような理由から，これらの手法を実用的な半構造データベースに応用することは困難であった．そのため我々は，論文 [7] において，XPress の手法を改良して，データ検索の能力を向上させることに成功した．さらに，そのことによる検索速度の落ち込みも回避しているため，検索能力は XPress を上回っているといえる．

3 ビット並列化

ビット並列化と呼ばれる手法は，非決定性の有限オートマトンの状態をビットベクトルでコンパクトに表現し，AND や OR, NOT といったビッ

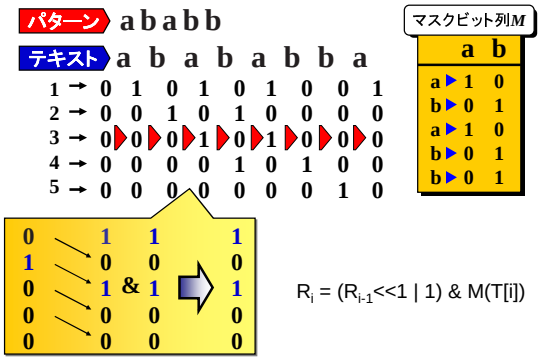


図 2.2: ビット並列化の手法．テキスト文字列 abababba に対してパターン文字列 ababb を検索する様子．

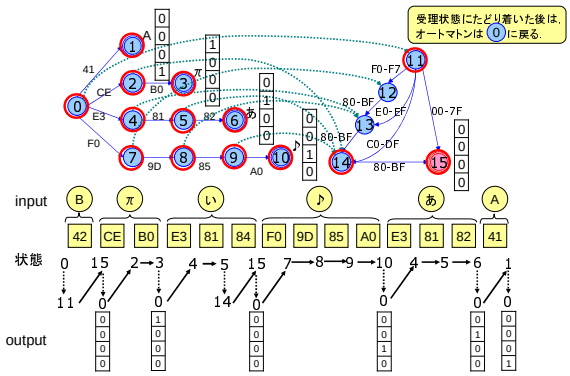


図 2.3: パターン集合 $P = \{$ π, あ, ♪,A$\}$ に対するコードオートマトン（UTF-8）．

ト演算を駆使することによって状態遷移を高速に実現する手法である（図 2.2）．これまでにも通常の文字列照合のみならず，近似文字列照合や正規表現へのマッチングなどへの応用が知られている．特に，32 ビットや 64 ビットの CPU が普及し，また MMX や SSE といったベクトル命令によって一度に多くのビット演算を行うことが容易になるにつれ，より大きなサイズの有限オートマトンを表現でき，また複雑な操作が可能になることから，より注目が高まっている．しかしながら，これまでは，いずれも英文テキストや遺伝子配列などのようにアルファベットサイズが小さい場合にその応用が限られており，日本語テキストのように複数バイトの文字列に対しては適用が困難であった．これは，それぞれの文字に対応させたビットマスクを用意する必要があるためであり，そのまま日本語テキストに対して適用するには領域効率が悪すぎるのが問題になるからである．そこで本研究では，複数バイトのテキストをそのまま走査する有限オートマトンを考え，(図 2.3）直接その上で照合を行う方式を採用することによって，複数バイト文字列でもビット演算手法が有用であることを示した [4]．

また，挿入と削除のみを許した枠組みでの近似文字列照合アルゴリズムについて，ビット演算を活用した新たなアルゴリズムの開発に成功した [3]．

4 パターン発見アルゴリズムの開発

文字列集合 S と T が与えられたときに，S と T を弁別するための特徴付けを行うパターンを，文字列パターンとして発見する問題は，機械学習や機械発見の研究において中心的な課題のひとつになっている．我々は，弁別の度合いを表すスコア関数を導入し，これを最適化問題として取り組んでいる．この際，特徴付けに使うパターンの複雑さによって，その計算時間は大きく異なる．一般に，複雑なパターンを用いることによって表現力が上がるが，その代償として，探索空間が増大するために，スコアを最大にするパターンを見つけるための計算量も上がる．したがって，適度な表現力をもつパターンを高速に見つけ出すアルゴリズムとそれを支えるデータ構造の開発が重要な研究課題となる．この研究課題に対する我々のこれまでの一連の成果をまとめたものを国際会議の招待講演で発表した [11]．

これまでは，主にひとつのパターンを用いて特徴付けを行ってきたが，今年度はさらに，複数のパターンの組み合わせによる表現力の向上に取り組んだ．もちろん，この際に重要になるのは飛躍的に増大する探索空間に対する対処である．我々は，２つの部分文字列パターン p と q を AND, OR, NOT を任意に組み合わせて得られるパターン表現（例えば $p \wedge q$ や $p \vee \neg q$ など）に対して，$O(N^2)$ 時間で最適なものを見つけ出すアルゴリズムの開発を行った [1, 2]．ここで N は入力として与えられた文字列集合の長さの総和である．このアルゴリズムは，接尾辞木と呼ばれるデータ構

造を用いたものである．接尾辞木は，与えられた文字列集合の中に現れるすべての接尾辞をパスとしてもつ木構造であり，文字列処理の分野でよく用いられている．領域使用量は，表そうとする文字列集合の長さの総和の線形サイズで収まり，また線形時間の構築アルゴリズムも知られているため，大変有用である．しかしながら，線形サイズとはいえ，その定数項が小さくないため，大規模な文字列集合を表す際にはそれが現実的な問題となりうる．そこで我々は，より領域使用量の少ない，接尾辞配列と呼ばれるデータ構造を用いて，仮想的に接尾辞木上でのアルゴリズムを模倣することによって，より実用性の高いアルゴリズムも与えた．

上述した複数のパターンの組み合わせによる表現を考える際に，対象とする文字列集合の個々の文字列の長さが比較的短い場合には顕在化しないが，長い文字列を対象にする場合には，そのパターンの出現場所が問題になってくる．特に，遺伝子配列データなど数百〜数千の長さの文字列に対してパターンの組み合わせを考える場合，パターン p の出現位置とパターン q の出現位置があまりにも離れている場合には，それらの組み合わせを考慮する効果に疑問が生じる．そこで我々は，パターンの出現位置の相対距離による制限を自由に与えることによって，この問題に対処することにした．ここでは，$p \wedge_\alpha q$ および $p \wedge_\alpha \neg q$ という 2 種類の組み合わせを対象とした．これらはそれぞれ，パターン p の出現位置から距離 α 以内の位置にパターン q が現れること，およびパターン p の出現位置から距離 α 以内の位置にはパターン q が現れないことを表すものであり，いずれも遺伝子情報処理において有用だと考えられる表現である．この問題に対して，$O(N^2)$ 時間，$O(N)$ 領域で最適のパターンの組み合わせを見つけ出すアルゴリズムを与えた [5]．そしてこれらのアルゴリズムを実装して成果を実証した．

5　今後の課題

今年度行ってきた研究は，主に文字列を対象としたものであった．次年度以降は，ここで得られた知見に基づきながら，木構造やグラフ構造といったより高次のデータ構造に対する拡張の可能性を探っていく予定である．また，その適用範囲を広げ，画像処理などへの応用も目指す．

参考文献

[1] H. Bannai, H. Hyyrö, A. Shinohara, M. Takeda, K. Nakai, and S. Miyano. Finding optimal pairs of patterns. In *Proc. 4th Workshop on Algorithms in Bioinformatics (WABI2004)*, volume 3340 of *Lecture Notes in Bioinformatics*, pages 450–452. Springer-Verlag, 2004.

[2] H. Bannai, H. Hyyrö, A. Shinohara, M. Takeda, K. Nakai, and S. Miyano. An $O(N^2)$ algorithm for discovering optimal boolean pattern pairs. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 1(4):159–170, 2004.

[3] H. Hyyrö, Y. Pinzon, and A. Shinohara. Fast bit-vector algorithms for approximate string matching under indel-distance. In *Proc. 31st Annual Conference on Current Trends in Theory and Practice of Informatics (SOFSEM2005)*, volume 3381 of *Lecture Notes in Computer Science*, pages 380–384. Springer-Verlag, 2004.

[4] H. Hyyrö, J. Takaba, A. Shinohara, and M. Takeda. On bit-parallel processing of multibyte text. In *Proc. The First Asia Information Retrieval Symposium (AIRS 2004)*, volume 3411 of *Lecture Notes in Computer Science*, pages 289–300. Springer-Verlag, 2004.

[5] S. Inenaga, H. Bannai, H. Hyyrö, A. Shinohara, M. Takeda, K. Nakai, and S. Miyano. Finding optimal pairs of cooperative and competing patterns with bounded distance. In *Proc. 7th International Conference on Discovery Science (DS 2004)*, volume 3245 of *Lecture Notes in Artificial Intelligence*, pages 32–46. Springer-Verlag, 2004.

[6] S. Inenaga, A. Shinohara, and M. Takeda. An efficient pattern matching algorithm on a subclass of context free grammars. In *Proc. 8th International Conference on Developments in Language Theory (DLT2004)*, volume 3340 of *Lecture Notes in Computer Science*, pages 225–236. Springer-Verlag, 2004.

[7] T. Maita and H. Sakamoto. A simple extension of queriable compression for XML data. In *Proc. the 2005 International Conference on Active Media and Technology*, 2005.

[8] M. Miyazaki, A. Shinohara, and M. Takeda. An improved pattern matching algorithm for strings in terms of straight line programs. *J. Disc. Algo.*, 1(1):187–204, 2000.

[9] H. Sakamoto. A fully linear-time approximation algorithm for grammar-based compression. *Journal of Discrete of Algorithm*, 2005.

[10] H. Sakamoto, T. Kida, and S. Shimozono. A space-saving linear-time algorithm for grammar-based compression. In *Proc. 11th International Symposium on String Processing and Information Retrieval (SPIRE2004)*, volume 3246 of *Lecture Notes in Computer Science*, pages 218–229. Springer-Verlag, 2004.

[11] A. Shinohara. String pattern discovery. In *Proc. 15th International Conference Algorithmic Learning Theory (ALT2004)*, volume 3244 of *Lecture Notes in Computer Science*, pages 1–13. Springer-Verlag, 2004.

[12] T. Suga and S. Shimozono. Approximate point set pattern matching on sequences and planes. In *Proc. 15th Annual Symposium on Combinatorial Pattern Matching (CPM 2004)*, volume 3109 of *Lecture Notes in Computer Science*, pages 89–101. Springer-Verlag, 2004.

研究業績一覧

学術論文

1. T. Suga and S. Shimozono:
"Approximate Point Set Pattern Matching on Sequences and Planes", Proc. 15th Annual Symposium on Combinatorial Pattern Matching (CPM 2004), Lecture Notes in Computer Science 3109, pp. 89–101, July 2004.
概要: The point set pattern matching problem is, given two sets "pattern" and "text" of points in Euclidean space, to find a linear transformation that maps the pattern to a subset of the text. We introduce an approximate point set pattern matching for axis-sorted point sequences that allows a translation, space insertions and deletions between points. We present an approximate pattern matching algorithm that runs with pattern size n and text size m in $O(nm^2)$ time in general, and in $O(nm)$ time if distances between two contiguous points in texts and patterns are finite. A variant of the four-Russian technique achieving $O(nm/\log n + n \log n)$ time is also provided. Furthermore, as a natural extension we present an approximate point set pattern matching on the plane, and give a polynomial-time algorithm that solves this problem.

2. S. Inenaga, A. Shinohara, and M. Takeda:
"A Fully Compressed Pattern Matching Algorithm for Simple Collage Systems", Proc. The Prague Stringology Conference'04 (PSC'04), Czech Technical University Press, pp. 98–113, September 2004.
概要: We study the fully compressed pattern matching problem (FCPM problem): Given T and P which are descriptions of text T and pattern P respectively, find the occurrences of P in T without decompressing T or P. This problem is rather chal-

lenging since patterns are also given in a compressed form. In this paper we present an FCPM algorithm for simple collage systems. Collage systems are a general framework that can represent various kinds of dictionary-based compressions, and simple collage systems are a subclass that includes LZW and LZ78 compressions. Collage systems are of the form $\langle D, S\rangle$, where D is a dictionary and S is a sequence of variables from D. Our FCPM algorithm performs in $O(||D||^2 + mn \log |S|)$ time, where $n = |T| = ||D|| + |S|$ and $m = |P|$. This is faster than the previous best result of $O(m^2n^2)$ time.

3. H. Bannai, H. Hyyrö, A. Shinohara, M. Takeda, K. Nakai, and S. Miyano:
"Finding Optimal Pairs of Patterns", Proc. 4th Workshop on Algorithms in Bioinformatics (WABI2004), Lecture Notes in Bioinformatics 3240, pp. 450–452, September 2004.
概要: We consider the problem of Finding the optimal pair of string patterns for discriminating between two sets of strings, i.e. finding the pair of patterns that is best with respect to some appropriate scoring function that gives higher scores to pattern pairs which occur more in the strings of one set, but less in the other. We present an $O(N^2)$ time algorithm for finding the optimal pair of substring patterns, where N is the total length of the strings. The algorithm looks for all possible Boolean combination of the patterns, e.g. patterns of the form $p \wedge \neg q$, which indicates that the pattern pair is considered to match a given string s, if p occurs in s, AND q does NOT occur in s. The same algorithm can be applied to a variant of the problem where we are given a single set of sequences along with a numeric attribute assigned to each sequence, and the problem is to find the optimal pattern pair whose occurrence in the sequences is correlated with this numeric attribute. An efficient implementation based on suffix arrays is presented, and the algorithm is applied to several nucleotide sequence datasets of moderate size, combined with microarray gene expression data, aiming to find regulatory elements that cooperate, complement, or compete with each other in enhancing and/or silencing certain genomic functions.

4. S. Inenaga, H. Bannai, H. Hyyrö, A. Shinohara, M. Takeda, K. Nakai, and S. Miyano:
"Finding Optimal Pairs of Cooperative and Competing Patterns with Bounded Distance", Proc. 7th International Conference on Discovery Science (DS 2004), Lecture Notes in Artificial Intelligence 3245, pp. 32–46, October 2004.
概要: We consider the problem of discovering the optimal pair of substring patterns with bounded distance α, from a given set S of strings. We study two kinds of pattern classes, one is in form $p \wedge_\alpha q$ that are interpreted as cooperative patterns within α distance, and the other is in form $p \wedge_\alpha \neg q$ representing competing patterns, with respect to S. We show an efficient algorithm to find the optimal pair of patterns in $O(N^2)$ time using $O(N)$ space. We also present an $O(m^2N^2)$ time and $O(m^2N)$ space solution to a more difficult version of the optimal pattern pair discovery problem, where m denotes the number of strings in S.

5. A. Shinohara:
"String Pattern Discovery", Proc. 15th International Conference Algorithmic Learning Theory (ALT2004), Lecture Notes in Artificial Intelligence 3244, pp. 1–13, October 2004.
概要: Finding a good pattern which discriminates one set of strings from the other set is a critical task in knowledge discovery. In this paper, we review a series of our works concerning with the string pattern

discovery. It includes theoretical analyses of learnabilities of some pattern classes, as well as development of practical data structures which support efficient string processing.

6. H. Sakamoto, T. Kida, and S. Shimozono: "A Space-Saving Linear-Time Algorithm for Grammar-Based Compression", Proc. 11th International Symposium on String Processing and Information Retrieval (SPIRE2004), Lecture Notes in Computer Science 3246, pp. 218–229, October 2004.
概要: A space-efficient linear-time approximation algoirithm for the grammar-based compression problem, which requests for a given string to find a smallest context-free grammar deriving the string, is presented. The algorithm consumes only $O(g_* \log g_*)$ space and achieves the worst case approximation ratio $O(\log g_* \log n)$, with the size n of an input and the optimum grammar size g_*. Experimental results for typical benchmarks demonstrate that our algorithm is practical and efficient.

7. H. Bannai, H. Hyyrö, A. Shinohara, M. Takeda, K. Nakai, and S. Miyano: "An $O(N^2)$ Algorithm for Discovering Optimal Boolean Pattern Pairs", IEEE/ACM Transactions on Computational Biology and Bioinformatics, Vol. 1, No. 4, pp. 159–170, December, 2004.
概要: We consider the problem of finding the optimal combination of string patterns, which characterizes a given set of strings that have a numeric attribute value assigned to each string. Pattern combinations are scored based on the correlation between their occurrences in the strings and the numeric attribute values. The aim is to find the combination of patterns which is best with respect to an appropriate scoring function. We present an $O(N^2)$ time algorithm for finding the optimal pair of substring patterns combined with Boolean functions, where N is the total length of the sequences. The algorithm looks for all possible Boolean combinations of the patterns, e.g., patterns of the form $p \wedge \neg q$, which indicates that the pattern pair is considered to occur in a given string s, if p occurs in s, AND q does NOT occur in s. An efficient implementation using suffix arrays is presented, and we further show that the algorithm can be adapted to find the best *k-pattern* Boolean combination in $O(N^k)$ time. The algorithm is applied to mRNA sequence data sets of moderate size combined with their turnover rates for the purpose of finding regulatory elements that cooperate, complement, or compete with each other in enhancing and/or silencing mRNA decay.

8. H. Hyyrö, J. Takaba, A. Shinohara, and M. Takeda:
"On Bit-Parallel Processing of Multibyte Text", Proc. The First Asia Information Retrieval Symposium (AIRS 2004), Lecture Notes in Computer Science 3411, pp. 289–300, February 2005.
概要: There exist practical bit-parallel algorithms for several types of pair-wise string processing, such as longest common subsequence computation or approximate string matching. The bit-parallel algorithms typically use a size-σ table of match bit-vectors, where the bits in the vector for a character λ identify the positions where the character λ occurs in one of the processed strings, and σ is the alphabet size. The time or space cost of computing the match table is not prohibitive with reasonably small alphabets such as ASCII text. However, for example in the case of general Unicode text the possible numerical code range of the characters is roughly one million. This makes using a simple table impractical. In this paper we evaluate three different schemes for over-

coming this problem. First we propose to replace the character code table by a character code automaton. Then we compare this method with two other schemes: using a hash table, and the binary-search based solution proposed by Wu, Manber and Myers. We find that the best choice is to use either the automaton-based method or a hash table.

9. S. Inenaga, A. Shinohara, M. Takeda:
"An Efficient Pattern Matching Algorithm on a Subclass of Context Free Grammars", Proc. 8th International Conference on Developments in Language Theory (DLT2004), Lecture Notes in Computer Science 3340, pp. 225–236, December 2004.
概要: There is a close relationship between formal language theory and data compression. Since 1990's various types of grammar-based text compression algorithms have been introduced. Given an input string, a grammar-based text compression algorithm constructs a context-free grammar that only generates the string. An interesting and challenging problem is pattern matching on context-free grammars $\mathcal{P}$ of size m and $\mathcal{T}$ of size n, which are the descriptions of pattern string P of length M and text string T of length N, respectively. The goal is to solve the problem in time proportional only to m and n, not to M nor N. Kieffer et al. introduced a very practical grammar-based compression method called multilevel pattern matching code (MPM code). In this paper, we propose an efficient pattern matching algorithm which, given two MPM grammars $\mathcal{P}$ and $\mathcal{T}$, performs in $O(mn^2)$ time with $O(mn)$ space. Our algorithm outperforms the previous best one by Miyazaki et al. which requires $O(m^2n^2)$ time and $O(mn)$ space.

10. H. Hyyrö, Y. Pinzon and A. Shinohara:
"Fast Bit-Vector Algorithms for Approximate String Matching under Indel-Distance", Proc. The 31st Annual Conference on Current Trends in Theory and Practice of Informatics (SOFSEM2005), Lecture Notes in Computer Science 3381, pp. 380–384, January 2005.
概要: The approximate string matching problem is to find all locations at which a query p of length m matches a substring of a text t of length n with at most k differences (insertions, deletions, substitutions). The fastest solutions in practice for this problem are the bit-parallel NFA simulation algorithms of Wu & Manber and Baeza-Yates & Navarro, and the bit-parallel dynamic programming algorithm of Myers. In this paper we present modified versions of these algorithms to deal with the restricted case where only insertions and deletions (called indel for short) are permitted. We also show test results with the algorithms.

11. H. Sakamoto:
"A Fully Linear-Time Approximation Algorithm for Grammar-Based Compression", Journal of Discrete of Algorithm, （掲載予定）.
概要: A linear-time approximation algorithm for the *grammer-based compression* is presented. This is an optimization problem to minimize the size of a context-free grammar deriving a given string. For each string of length n, the algorithm guarantees $O(\log \frac{n}{g_*})$ approximation ratio without suffix tree construction.

12. T. Maita and H. Sakamoto:
"A Simple Extension of Queriable Compression for XML Data", Proc. the 2005 International Conference on Active Media and Technology, （掲載予定）.
概要: Recently, the method of reverse arithmetic encoding for effective compression and fast query process for semi-structured

data was proposed. We apply this method and develop a new method for more complicated query process. By the reverse arithmetic encoding, we can check the dependency between any two paths without decoding and using this property, a fast query process over tree structures is obtained. However, it is difficult to handle general queries since the type of query is very restricted. So, we expand the algorithm to realize the Boolean operations "NOT" and "OR" in the query expressions.

A10: 変移する要素間の関係を条件とする組合せ最適化モデル

宮野 英次 † 朝廣 雄一 ‡

† 九州工業大学情報工学部
〒 820-8502 福岡県飯塚市川津 680-4
miyano@ces.kyutech.ac.jp

‡ 九州産業大学 情報科学部
〒 813-8503 福岡県福岡市東区松香台 2-3-1
asahiro@is.kyusan-u.ac.jp

1 研究目的

現実世界に現れる多くのシステム工学的，情報工学的問題は，離散的な構造を有しており，組合せ計画モデルとして定式化できる場合が多い．代表的なものとしては，知的交通システムにおける車両配送計画やビジネス・プロセス・フロー設計などが挙げられる．例えば，車両配送計画を従来の数理計画モデルに従って定式化する場合には，車両台数，運搬量，配送コスト，締め切り等の制約となる属性パラメータ値を入力要素として捉え，完全かつ固定的に，与えられた要素間の関係ならびに制約条件を数式化する．配送計画作成アルゴリズムは，すべての制約条件を完全に満足する最適解，あるいは処理時間を優先する場合には準最適解（近似解）を求めるように設計される．得られた解の精度・処理時間に違いはあるものの，いずれの場合も事前に作成した条件に基づき作業計画を決定することになる．

しかし，近年の社会環境の変化は著しく，時間をかけて作成した完全な作業計画が時をおかずに陳腐化してしまうという状況があり，従来の固定的に制約が与えられる計算モデルでは対応できないという問題が生じている．そのため，本研究では，入力要素の値が時間とともに連続的に変移する環境において，要素間の関係が時々刻々と変化するような様々な問題を扱い，数理最適化モデルとして定式化する統一的な手法の検討と，精度の高い近似解及び高速性能を保証するアルゴリズムの開発を目的とする．

2 移動系における組合せ最適化問題

今年度は，固定的に制約が与えられる従来の車両配送計画問題を拡張して，移動系における組合せ最適化問題としてモデル化し，本問題に対するアルゴリズムの設計と計算量に関する検討を行った．

2.1 問題の形式的定義と結果概要

次のような実用場面で現れるロボット・アームの行動スケジュールを考える．ベルトコンベアの上に置かれた荷物が与えられたとき，ロボット・アームは移動する荷物を掴み，回収点へと運ぶ動作を繰り返し，できるだけ多くの荷物を回収することを目標とする．このような問題を，移動系に対する回収問題 (Maximum k-Collect Tours for Moving Objects，以下 MAX-kCT 問題) として形式化を行った．

MAX-kCT 問題： 初期入力として，ユークリッド平面上に，回収者 (ロボット・アーム)$A(k)$ と n 個の移動物体 $b_i \in B$ $(i = 1, \cdots, n)$ が与えられる．回収者 $A(k)$ は回収容量 k を持ち，初期位置は回収点 (原点) とする．1 回の回収では最大 k 個までしか回収できないため，それ以上回収するためには，回収点へ一旦戻り再び回収に向かう必要がある．回収者は任意の方向に移動可能で，常に速さ $v(A(k))$ で等速運動をしているか速さ 0 で停止しているかのどちらかであり，方向転換や移動物体回収の際に速さが落ちることはないものとする．移動物体 b_i は，初期位置 $(x(b_i), y(b_i)) \in R^2$ と経路 $trace(b_i)$ が与えられ，速さ $v(b_i)$ で等速運動するが，時刻 $release\ time$ $r(b_i)$ から回収可能となり時刻 $deadline$ $d(b_i)$ で回収不可能となる．このとき，回収動作を繰り返すことにより，移動物体を最大個回収する経路 P を求める問題を考える．

すべての物体が動かず，回収者の容量 $k \geq n$ の場合は，Deadline-TSP 問題 [2] (または Vehicle Routing with Time Windows 問題 [8, 7]，Orienteering 問題 [4]) として知られている．この問題は $\mathcal{NP}$ 困難であり，一般化された問題を解くことは非常に困難である．また，本問題は，組合せ最適化問題である巡回セールスマン問題 (Traveling Sales Person Problem，以下 TSP) の応用とも言える．TSP は，最も有名な $\mathcal{NP}$ 困難問題であり，さまざまなヒューリスティック法や近似アルゴリズムが考えられている．また，最近では，移動系における TSP 問題である，Dynamic k-Collect TSP 問題 [5]，Moving-Target TSP 問題 [10]，Kinetic TSP 問題 [9] などが考えられている．これらの問題は，容量 k の回収者 $A(k)$ と n 個の移動物体 b_j が与えられ，回収者の速さ $v(A)$ と移動物体の速さ $v(b_j)$ の関係が，全ての移動物体に対して $v(A) > v(b_j)$ である，つまりどの移動物体よりも回収者が速いとき，全ての移動物体を最短距離で回収する問題であり，本研究課題でモデル化を行った最大化問題とは異なることに注意する．Chalasani らは $k = \infty$ のとき，定数近似アルゴリズムを提案し，さらに $k = 1$ の回収者と移動物体が 1 本の線上を移動する場合は多項式時間で解けることを示した [5]．また，Helvig らは $k = \infty$ で，さらに高々 $O(\frac{\log n}{\log \log n})$ 個の移動物体が移動しているときは，$(1+\sigma)$-近似アルゴリズムがあることを示した [10]．ここで σ は従来の TSP に対する近似率を表す．Hammar と Nilsson は $k = \infty$ で全ての移動物体が同じ速さで移動するとき，PTAS であることを示した [9]．最大化問題としてのモデル化については，朝廣および領域内研究者によるものしか見られない [1].

今年度は，荷物の回収期限である *release time* と *deadline* が一般の場合について検討を行った．また，回収容量 $k = 1$ とした問題 MAX-1CT を中心に考えた．本研究課題における主要な結果は以下である： (i) MAX-1CT で，移動物体を直線上のみ移動するとした問題 MAX-1CT on Lines は $\mathcal{NP}$ 困難となる．(ii) しかし，全ての移動物体が回収者よりも速く移動する場合については，下側エンベロープを利用した，移動物体を取って原点へ戻る時間が最小のものを毎回取るという貪欲戦略に基づくアルゴリズムを用いることによって，$O(n\alpha(n)\log n)$ の計算時間で回収することが可能である．ここで，$\alpha(n)$ は Ackermann 関数の逆関数である．(iii) MAX-1CT で，移動物体が原点を中心とする同心円上を描く軌道上を移動するとした問題 MAX-1CT on Circles は，代表的なスケジューリング問題である仕事割当区間スケジューリング問題 (Job Interval Scheduling Problem，JISP) [3, 6] から帰着できるため，この場合も $\mathcal{NP}$ 困難となる．このとき，JISP の 1.582-近似アルゴリズム [6] を用いることで，同様に MAX-1CT on Ciecles に対する近似アルゴリズムを設計することができる．

2.2 直線上の移動物体が速い場合

移動物体 b_i が直線 $l(b_i)$ 上を動く場合について検討を行った．このように移動に制限を加えた問題を “MAX-kCT on Lines” とする．まず，MAX-1CT on Lines において，移動物体が回収者よりも速い，すなわち $v(b_i) \geq v(A(1))$ である場合を考える．この問題は次のような貪欲アルゴリズムで解くことができる： 時刻 t に回収者 $A(1)$ が原点を出発し，移動物体 b_i を回収した後，再び原点へ戻ったときの時刻を *compleation time* $T_i(t)$ とする．回収者は原点を出発するときに，この $T_i(t)$ が最小のものを毎回に取りにいくことで，移動物体を最大個回収できる．

結果 1． MAX-1CT on Lines で全ての移動物体が回収者よりも速い場合において，移動物体を最大個回収する $O(n^2)$ のアルゴリズムが存在する．

さらに下側エンベロープを用いることで MAX-1CT on Lines の計算時間の上限を下げることができる．$f_i(t)$ は範囲 $[r(b_i), d(b_i)]$ の連続関数であり，$\mathcal{F} = \{f_1(t), f_2(t), \cdots, f_n(t)\}$ と定義すると，$\mathcal{F}$ の下側エンベロープは次のように定義される．

$$E_{\mathcal{F}(t)} = \min_{1 \leq i \leq n} f_i(t)$$

Algorithm Envelope:

Stage 1. 全ての移動物体 b_i に対して，$f_i(t)$ を計算する．

Stage 2. $\mathcal{F} = \{f_1(t), f_2(t), \cdots, f_n(t)\}$ に対する下側エンベロープ $E_{\mathcal{F}}$ を計算する．

Stage 3. 時刻 $t = 0$ とし，原点にいる回収者が取ることのできる移動物体が存在する間，以下の動作を繰り返す．

3-1. 下側エンベロープ $E_{\mathcal{F}}$ で求めた，現時刻 t で最短時間 $f_{min}(t)$ で回収可能な移動物体 b_{min} を回収し，原点へ戻る．

3-2. $t = f_{min}(t)$，$P = P \cup b_{min}$ と更新する．

Stage 4. 取った移動物体 $P = \{p_1, p_2, \cdots, p_j\}$ を出力し終了する．

結果 2． どの移動物体も回収者より速い場合の MAX-1CT において，移動物体を最大個回収する $O(n\alpha(n)\log n)$ アルゴリズムが存在する．このとき，$\alpha(n)$ は *Ackermann* 逆関数である．

2.3 直線上の移動物体が遅い場合

MAX-kCT on Lines に制限を加えない，一般的な問題に対する計算複雑さに関して以下のような結果を得た．

結果 3． (i) MAX-1CT on Lins は $\mathcal{NP}$ 困難である．従って，(ii) MAX-kCT on Lines も $\mathcal{NP}$ 困難である．

証明 ： MAX-kCT は最大化問題であるため，決定問題として，回収者の容量 k としたとき m 個以上の移動物体を取ることができるかを問う，MAX-kCT(m) として考える．

まず，MAX-kCT(m) $\in \mathcal{NP}$ を示す．今，MAX-kCT(m) の各パラメータと整数 m が与えられたとする．ここで選ぶ証明書は移動物体を取った経路 P である．検証アルゴリズムは，$|P| = m$ を確認し，経路 P で得られた各移動物体 b_i を取る時刻 t に，取って戻る時間 $f_i(t)$ で取って戻ることができるかどうかを調べれば良い．あらかじめ与えられた経路の式に時刻を代入し検証するだけなので，この検証は多項式時間で実現できる．よって MAX-kCT(m) $\in \mathcal{NP}$ である．

次に $\mathcal{NP}$ 完全である瓶詰め問題 (Bin Packing 問題，以下 BP) から，回収者の容量 $k = 1$ とした問題である MAX-1CT(m) on Lines に帰着させる．つまり $BP \leq p$MAX-1CT(m) on Lines を示し，MAX-1CT(m) が $\mathcal{NP}$ 完全であることを示す．BP は次のように定式化される．

BP: n 個の品物 $I = \{i_1, i_2, \cdots, i_n\}$ があり，それぞれ大きさ $size(x_i)$ をもっている．容量 γ の瓶があり，瓶の容量を越えて品物をつめこむことはできない．このようなときに，λ 個以下の瓶に品物を全てつめこむ問題を考える．

帰着を行うにあたって一般性を損なわないように，BP の品物の大きさを $size(i_1) \leq size(i_2) \leq \cdots \leq size(i_n)$ とする．

まず，図 2.1 のような MAX-1CT(m) on Lines を考える．容量 $k = 1$ の回収者の速さ $v(A) = 1$ とする．*release line* と *deadline line* の 2 つの辺を原点 $O(0,0)$ から引く．*release line* の角度 θ_r は $\frac{\pi}{2} < \theta_r < \pi$ で，*deadline line* の角度 θ_d は $\theta_d = \pi - \theta_r$ である．ここで，BP において与えられた品物の数 n と瓶の数 λ を，MAX-1CT(m) on Lines では n 個の移動物体 $b_1, b_2, \cdots, b_n$ に加え，$(\lambda - 1)$ 個の特殊な移動物体 $b_{n+1}, b_{n+2}, \cdots, b_{n+(\lambda-1)}$ に対応させる．移動物体 b_j $(1 \leq j \leq n+(\lambda-1))$ は，*release time* である時刻 $r(b_j)$ に初期位置 $(x(b_j), y(b_j))$ から回収可能となり，そのまま x 軸と平行に速さ $v(b_j)$ で *deadline* である時刻 $d(b_j)$ になるまで移動し続ける．つまり，移動物体 b_j の移動する軸 $l(b_j)$ は初期位置 $(x(b_j), y(b_j))$ を通る x 軸に平行な直線である．$(x(b_j), y(b_j)), r(b_j), d(b_j), v(b_j)$ については，以下の通りに定義される．

(i) b_j $(1 \leq j \leq n)$ の移動物体について

- 初期位置：
  $(x(b_j), y(b_j)) = (\frac{size(i_j)}{2}\cos\theta_r, \frac{size(i_j)}{2}\sin\theta_r)$
- *release time*： $r(b_j) = 0$
- *deadline*： $d(b_j) = n \times \gamma + (\lambda - 1)$
- 移動物体の速さ： $v(b_j) = \frac{-size(i_j)\cdot\cos\theta_r}{n\times\gamma+(\lambda-1)}$

(i) の移動物体 b_j は，初期位置が *release line* 上にあり，*deadline* が *deadline line* に到着する時刻となっている．

(ii) $b_j = b_{n+s}$ $(1 \leq s \leq \lambda - 1)$ の移動物体について

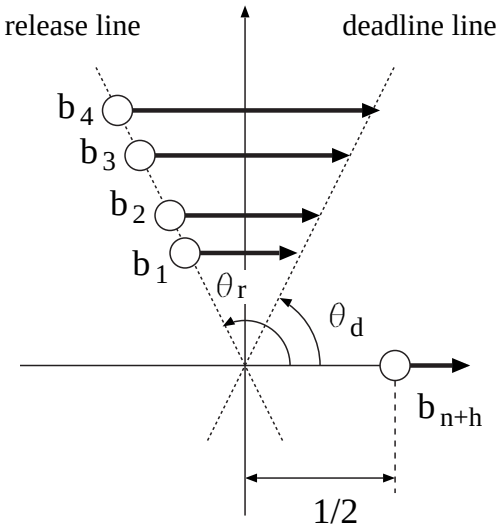


図 2.1: MAX-1CT(m) on Lines

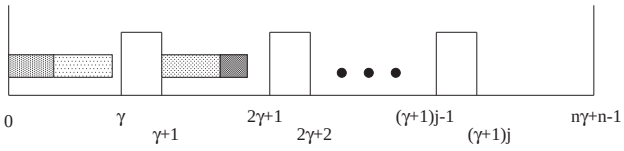


図 2.2: 移動物体を取って戻る時間のグラフ

- 初期位置： $(x(b_j), y(b_j)) = (\frac{1}{2}, 0)$
- *release time*： $r(b_j) = (\gamma + 1) \times s - \frac{1}{2}$
- *deadline*： $d(b_j) = (\gamma + 1) \times s$
- 移動物体の速さ： $v(b_j) = 1$

これらのときの $\theta_r (= \theta_d = \pi - \theta_d)$ を考える．回収者が移動物体を取りに行く時間を考えると，初期位置で取る際と y 軸上で取る場合には誤差が生じる．移動物体を取る順序だけを考慮すればいいように，この誤差が影響を及ぼさないように設定すると，以下の不等式が成り立つ．

$$(1 - \sin\theta_r) \cdot \sum_{i \in I} size(i) < 1$$

よって，この不等式を満たし，かつ $\frac{\pi}{2} < \theta_r < \pi$ にある θ_r を決める．

このような MAX-1CT(m) on Lines を考えたとき，次の補題を得る．

補題 1． *BP* の λ か，より少ない瓶の数が求まったとき，*BP* の各インスタンスを対応付けすることで，容量 $k = 1$ の回収者は $n + (\lambda - 1)$ 個の移動物体全てを回収することができる．

証明： $n + (\lambda - 1)$ 個の移動物体を集める手順を示す．そのためにまず，$b_j = b_{n+s}$ $(1 \le s \le \lambda - 1)$ の全ての移動物体は，取れる時刻が限られているため取る時間がすぐに決まる事を示し，それらの移動物体を取る作業の間に残りの b_j $(1 \le j \le n)$ の移動物体を対応する *BP* の品物の順に取っていけば全ての移動物体を取ることができることを示す (図 2.2)．

(i) $b_j = b_{n+s} (1 \le s \le \lambda - 1)$ の移動物体について

はじめに，回収者 $A(1)$ は時刻 γ に原点を出発し，x 軸に沿って移動して，移動物体 b_{n+1} を時刻 $r(b_{n+1}) = (\gamma + 1) - \frac{1}{2})$ に $(x(b_{n+1}), y(b_{n+1}))$ で取り，時刻 $(\gamma + 1)$ に原点へ戻る．$2 \le s \le (\lambda - 1)$ の移動物体に対しても同様に，$A(1)$ は時刻 $s \cdot (\gamma + 1) - 1$ に原点を出発し，x 軸に沿って移動して，移動物体 b_{n+s} を時刻 $r(b_{n+s}) = s \cdot (\gamma + 1) - \frac{1}{2}$ に $(x(b_{n+s}), y(b_{n+s}))$ で取り，時刻 $s \cdot (\gamma + 1)$ に原点へ戻る (図 2.2 参照)．よって，移動物体 b_{n+s} を取る時間帯は $[s \cdot (\gamma + 1) - 1,\ s \cdot (\gamma + 1)]$ となり，これらの移動物体を取る時間帯が重なることはない．このように $b_j = b_{n+s} (1 \le s \le \lambda - 1)$ の移動物体を取ることが最適解となる．

(ii) b_j $(1 \le j \le n)$ の移動物体について

(i) の移動物体の取り方を決めた後で (ii) の移動物体を取るものとして議論する．つまり，(ii) の移動物体は $[s \cdot (\gamma + 1) - 1,\ s \cdot (\gamma + 1)]$ $(1 \le s \le \lambda - 1)$ の間は取ることができない．つまり，それ以外の部分で，どのように取っていくかを考える必要がある．回収者 $A(1)$ は原点を出発し，ある移動物体 $b_j (1 \le j \le n)$ を 1 個取ったあと原点へ戻る．このときにかかる時間は，原点から移動物体の初期位置までの距離が $\frac{size(i_j)}{2}$ なので，最大 $size(i_j)$ かかる (図 2.1 参照)．つまり，原点から移動物体までの距離が最大値を取るのは，*release line* か *deadline line* 上にある場合である．

BP において，瓶 μ には品物 $\mathcal{I} = \{i_{\nu_1}, i_{\nu_2}, \cdots i_{\nu_\mu}\}$ $(\nu_1 \le \nu_2 \le \cdots \le \nu_\mu)$ が入る．これを使って回収者の動作を考えると次の通りになる．

Step 1 $(\mu-1)(\gamma+1)-1$ に原点を出発する．

Step 2 最短で b_{ν_1} を取れる位置に移動する．

Step 3 b_{ν_1} を取り原点へ戻る．

Step 4 Step 1 - 3 を繰り返し，$a \in \{\nu_2, \cdots, \nu_\mu\}$ を取り，時刻 $(\mu-1)(\lambda+1)-1+\sum_{e:e<a, i_e \in \mathcal{I}} size(i_e)$ に原点へ戻る．

回収者 $A(1)$ が，Step 2 と Step 3 で移動物体 b_{ν_1} を取って戻って来るのにかかる時間は，最大で $size(i_{\nu_1})$ かかる．他の移動物体 b_i $(i \in \mathcal{I})$ を取る最大時間も $size(i)$ である．BP においては，$\mathcal{I}$ の品物全てをある瓶 μ に入れることができるので，$\sum_{i \in \mathcal{I}} size(i) \leq \gamma$ である．同様にこの問題では，$i \in \mathcal{I}$ と対応する移動物体 b_i を取る区間を考えると，瓶 μ と対応する区間の範囲は $[(\mu-1)(\gamma+1)-1, (\mu-1)(\gamma+1)+\gamma-1]$ となっており，区間の大きさは γ なので，区間に入れていくことができる．

(i) と (ii) により，BP の λ が求まったとき，回収者 $A(1)$ は $n+(\lambda-1)$ 個の移動物体を集めることができる．(補題 1 の証明終り)

補題 2． *BP において，より少ない瓶の数 λ がわかっているときだけ．容量 $k=1$ の回収者 $A(1)$ は $n+(\lambda-1)$ 個の全ての移動物体を回収することができる．*

証明： BP の解である λ かより少ない瓶の数が求まっていないと仮定する．各 j について，$size(i_j)$ は整数なので，より有効な解では瓶の中の総量は少なくとも $\lambda+1$ は取れる．瓶の中の品物の集合を $\mathcal{I} = \{i_{\nu_1}, i_{\nu_2}, \cdots, i_{\nu_\mu}\}$ とする．それに対応する移動物体 $\mathcal{B} = \{b_{\nu_1}, b_{\nu_2}, \cdots, b_{\nu_\mu}\}$ を順次取っていくことを考える．全ての b_ν をそれぞれ最短時間 $size(i_\nu)$ で取って戻ったと考えると，

$$\begin{aligned} & \sum_{i \in \mathcal{I}} size(i_\nu) - \sum_{i \in \mathcal{I}} (size(i_\nu) \cdot \sin\theta_r) \\ = \ & (1-\sin\theta_r) \cdot \sum_{i \in \mathcal{I}} size(i_\nu) \\ \leq \ & (1-\sin\theta_r) \cdot \sum_{i \in \mathcal{I}} size(i) \\ < \ & 1 \end{aligned}$$

従って，長さ γ の間では $\mathcal{B}$ の移動物体の数より多く取ることができない．

次に b_{n+s} $(1 \leq s \leq \lambda-1)$ の移動物体を全て集めることについて考える．これらの移動物体は．$(\frac{1}{2}, 0)$ に出現し，その後 x 軸に沿って $x > \frac{1}{2}$ へ移動する．回収者 $A(1)$ が b_{n+s} を回収する場所は，$(x_{n+s}, 0)$ $(x_{n+s} \geq \frac{1}{2})$ である．$x_{n+s} > \frac{1}{2}$ のときの回収の流れは，回収者 $A(1)$ は原点を時刻 $r(b_{n+j}) - \frac{1}{2}$ 出発し，$(x_{n+s}, 0)$ へ移動した後，時刻 $d(b_{n+s})$ へ移動する．ここで，動き $\mathcal{M}$ を，$\mathcal{M}$ の手順で取れる移動物体 b_j $(1 \leq j \leq n)$ と同じで，時間帯 $[s \cdot (\gamma+1)-1, s \cdot (\gamma+1)]$ に移動物体 b_{n+s} が取れる動き $\mathcal{M}'$ に変換する．移動物体 b_j を集める経路 $\mathcal{M}$ と，それに対応する $\mathcal{M}'$ は時刻 $r(b_{n+s})$ に原点を出発し，$(\frac{1}{2}, 0)$ へ移動した後，時刻 $d(b_{n+s})$ に原点へ戻るものと定義される．この新しく定義された $\mathcal{M}'$ での動きを考えると，全ての $r(b_{n+s})$ は b_j $(1 \leq j \leq n)$ と重なることはなく，b_{n+s} を回収するときは，回収可能になる時刻ちょうどに取れるように $r(b_{n+s}) - \frac{1}{2}$ まで原点で待機する．このことから，$\mathcal{M}'$ で集められる移動物体の数は，$\mathcal{M}$ と同じであると推測する．

b_{n+s} $(1 \leq s \leq \lambda-1)$ の移動物体を全て集めることについて，動き $\mathcal{M}'$ は長さ γ の時間帯の収集だけを残すので，b_j $(1 \leq j \leq n)$ の移動物体を全て集めることはできない．(補題 2 の証明終り)

2 つの補題から，BP から MAX-1CT on Lines に帰着可能ということがわかる．よって MAX-1CT on Lines は $\mathcal{NP}$ 困難である．MAX-1CT は MAX-kCT の部分集合だから，MAX-kCT も $\mathcal{NP}$ 困難である．

2.4 曲線上の移動物体の場合

本節では，移動物体 b_i が原点を中心とする同心円 c_i 上を動く場合について考える．本問題を”MAX-1CT on Circles” とし，次の定理を得る．

結果 4． *(i)MAX-1CT on Circles は $\mathcal{NP}$ 困難である．したがって，(ii)MAX-kCT on Circle も $\mathcal{NP}$ 困難である．*

証明： MAX-1CT は最大化問題であるため，決定問題として，回収者の容量 1 のとき m 個以上の移

動物体を回収することができるかを問う，MAX-1CT(m) として考える．この証明では JISP 問題から帰着して考える [3, 6]．JISP はインスタンスとして，ジョブ job_i，*release time* r_i，*deadline* d_i，*processing time* t_i を持つ $(0 \leq i \leq n)$．ここで，移動物体 b_i をジョブ job_i，b_i の移動する円 c_i の半径を $\frac{t_i}{2}$，*release time* と *deadline* をそれぞれ r_i と d_i に対応付けすることで帰着することができる．

参考文献

[1] Y. Asahiro, T. Horiyama, K. Makino, H. Ono, T. Sakuma, M. Yamashita. How to collect balls moving in the Euclidean plane. *Elec. Notes in TCS*, 91, pp.229–245, 2004.

[2] N. Bansal, A. Blum, S. Chawla, A. Meyerson. Approximation algorithms for deadline-TSP and vehicle routing with time-windows. In *STOC*, pp.166–174, 2004.

[3] A. Bar-Noy, S. Guha, J. Naor, B. Schieber. Approximating the throughput of multiple machines under real-time scheduling. In *STOC*, pp.622–631, 1999.

[4] A. Blum, S. Chawla, D. Karger, T. Lane, A. Meyerson, M. Minkoff. Approximation algorithms for orienteering and discounted-reward TSP. In *FOCS*, pp.46–55, 2003.

[5] P. Chalasani, R. Motwani, A. Rao. Approximation algorithms for robot grasp and delivery. In *Proc. Int. Workshop on Algorithmic Foundations of Robotics*, pp.347–362, 1996.

[6] J.Chuzhoy, R. Ostrovsky, Y. Rabani. Approximation algorithms for the job interval selection problem and related scheduling problem. In *FOCS*, pp.348–356, 2001

[7] J.-F. Cordeau, G. Desaulniers, J. Desrosiers, M.M. Solomon, F. Soumis. VRP with time windows. In *The Vehicle Routing Problem*, P. Tosh and D. Vigo Eds., SIAM, 2002.

[8] M. Desrochers, J. Desrosiers, M.M. Solomon. A new optimization algorithm for the vehicle routing problem with time windows. *Operations Research*, 40, pp.342–354, 1992.

[9] M. Hammar and B.J. Nilsson. Approximation results for kinetic variants of TSP. In *ICALP*, pp.392–401, 1999.

[10] C.S. Helvig, G. Robins, A. Zelikovsky. Moving target TSP and related problems. In *ESA*, pp.453–464, 1998.

研究業績一覧

学術論文

1. Yuichi Asahiro, Eiji Miyano, Shinichi Shimoirisa:
"k-Collect Tours for Moving Objects with Release Times and Deadlines", Proceedings of the 9th World Multi-Conference on Systemics, Cybernetics and Informatics, (掲載予定).
概要: In this paper, we consider a formalization of the following scheduling problem motivated by a variety of practical applications: The input to the problem consists of a robot arm of capacity k (i.e., it can grasp at most k products at a time) and n products, each of which is associated with a release time and a deadline and moves on a predefined path with a fixed constant speed. In each round (tour), the robot arm grasps at most k products by their deadlines and delivers to a specified delivery point. The goal of the problem is to find a collection of tours such that the robot arm of capacity k grasps by their deadlines and delivers as many products as possible. In this paper we show that there is an $O(n\alpha(n)\log n)$ algorithm for the case $k = 1$ if all the products move on given straight lines with faster speeds than the robot arm, where $\alpha(n)$ is the inverse Ackermann function. However, for the similar setting for the paths of the products, we prove that if some of the products' speeds are slower than the robot arm's one, then the problem remains $\mathcal{NP}$-hard.

2. Yuichi Asahiro:
"Simple Greedy Methods for DNA Word Design", Proceedings of the 9th World Multi-Conference on Systemics, Cybernetics and Informatics, (掲載予定).
概要: For designing a large set of DNA strands, we tested three algorithms based on traditional greedy heuristics. The constraints to be considered for the set are Hamming Distance (HD) constraint, Reverse Complement (RC) constraint, and GC Content (GC) constraint. The variety of the combinations of these three constraints is the most fundamental target of designing DNA strands. By the algorithms, we found larger sets than previously known ones for some settings of the length n and Hamming Distance d, e.g., $n = 14$ and $d = 3, 10$ with HD, GC, and RC constraints, and $n = 12$ and $d = 5, 6, 7, 8$ with HD and RC constraints. In addition to that, the theoretical complexity of the problem is shown, which does not seem to be explained in the previous studies.

3. 下入佐真一，朝廣雄一，宮野英次:
"移動系における最大個数巡回アルゴリズム", 数理解析研究所講究録 (計算機科学基礎理論の新展開), 1375, pp.260–266, 2004 年 5 月.
概要: 平面上を移動する n 個の物体を巡回する経路選択問題に対して，次のような条件を付けた問題を考える．(i) n 個の物体の平面上での初期座標はあらかじめ与えられいる．(ii) 移動物体は一定の方向と一定の速さで等速直線移動しており，これらについてもあらかじめ与えられている．(iii) 巡回者の数は 1 とする．(iv) 巡回者は一定の速さで直線的に移動可能で，時間 0 で移動方向を換えることができる．例えば，一定の速度で生産ライン上を流れて来る部品を，ロボットアームにより加工する際の最適スケジュールなど，制御ロボットへの応用が考えられる．本稿では，巡回者の可動方向を 3 方向 (上下左) および 4 方向 (上下左右) とした場合に対する移動物体巡回問題を考える．また，巡回者と n 個の移動物体の速さはすべて等しく，移動物体の可動範囲は平行な 2 直線上に限られているとする．本稿では，巡回者が 4 方向に移動可能であるときに，巡回個数を最大とするような経路を求める $O(n + T_s(n))$ 時間アルゴリズムを示す．ここで $T_s(n)$ は n 要素のソーティングに必要な時間とする．また，巡回者の可動方向が 3 に制限した場合に n 個の移動物体を全て巡回可能か否かを判定する $O(n^3)$ 時間アルゴリズムが存在することを示す.

研究会等

1. Kazuo Iwama, Kousuke Izumi, Eiji Miyano, Hirotaka Ono:
"Drawing Borders Efficiently", 電子情報通信学会技術研究報告, 104 巻・147 号, pp.47–54, 2004 年 6 月.
概要: A spreadsheet, especially MS Excel, is probably one of the most popular software for personal-computer users and gives us convenient and user-friendly tools for drawing tables. In practical situations, we often wish to draw several vertical and horizontal black lines on selective gridlines to enhance the readability of our spreadsheet. Such situations we frequently encounter are formulated as the Border Drawing Problem (BDP). Given a layout of black line segments, from an algorithmic view point we study how to draw it efficiently by using a set of border styles and investigate its complexity. (i) We first give a formal model based on MS Excel, and then (ii) show that the problem is $\mathcal{NP}$-hard for the set of the Excel border styles and for any reasonable subset of the styles. Moreover, in order to provide potentially more efficient drawing, (iii) we propose a new compact set of border styles and show a necessary and sufficient condition of its drawability.

2. Kazuo Iwama, Kousuke Izumi, Eiji Miyano, Hirotaka Ono:
"Tiling Problems with the Edge-

Overwriting Rule", 情報処理学会研究報告, 2004 巻・101 号, pp.61–66, 2004 年 10 月.

概要: The tiling problems have received considerable attention for the last decades, and a lot of results are reported. One of the most popular variants of the problems could be tilings of regions with Wang tiles, which are 1×1 squares with colored edges, by using the following rule: If two tiles touch, then the color of their shared edges must be the same. In this paper, we consider a new tiling problem under the edge-overwriting rule in which any pair of tiles can touch but the color of the shared edges after tiling is determined by the edge color of the tile placed later. The problem input is a pair of a target figure and a tile set to be used, and the output is a sequence of tiles which realizes the target figure under the edge-overwriting rule. We show the sufficient and necessary condition of a tile set to realize any target figure, and then show $\mathcal{NP}$-hardness proof and an approximation algorithm for the problem of minimizing the number of tiles realizing target figures.

3. Yuichi Asahiro, Eiji Miyano, Shinichi Shimoirisa:
"Collect Tours for Moving Objects with Release Times and Deadlines", 電子情報通信学会技術研究報告, 104 巻・743 号, pp.79–85, 2005 年 3 月.

概要: In this paper, we consider a formalization of the following scheduling problem motivated by a variety of practical applications: The input to the problem consists of a robot arm of capacity k (i.e., it can grasp at most k products at a time) and n products, each of which is associated with a release time and a deadline and moves on a predefined path with a fixed constant speed. In each round (tour), the robot arm grasps at most k products by their deadlines and delivers to a specified delivery point. The goal of the problem is to find a collection of tours such that the robot arm of capacity k grasps by their deadlines and delivers as many products as possible. In this paper we show that there is an $O(n\alpha(n)\log n)$ algorithm for the case $k = 1$ if all the products move on given straight lines with faster speeds than the robot arm, where $\alpha(n)$ is the inverse Ackermann function. However, for the similar setting for the paths of the products, we prove that if some of the products' speeds are slower than the robot's one, then the problem is $\mathcal{NP}$-hard.

学会大会等

1. 下入佐真一，朝廣雄一，宮野英次:
"作業時間制約付き移動物体回収問題の $\mathcal{NP}$ 困難性", 電気関係学会九州支部連合大会講演論文集, 12-1A-01, 2004 年 9 月.

2. 池上佳一，宮野英次:
"三者が互いに関連付けられた間接認証方式の提案", 火の国情報シンポジウム 2005, 2005 年 3 月.

B01: 代数的および確率的手法による離散構造の限界の究明

伊東 利哉 † 上野 修一 ‡

† 東京工業大学 学術国際情報センター
〒 152-8550 東京都目黒区大岡山 2-12-1-E2-5
titoh@dac.gsic.titech.ac.jp

‡ 東京工業大学 大学院理工学研究科
〒 152-8552 東京都目黒区大岡山 2-12-1-S3-57
ueno@lab.ss.titech.ac.jp

1 緒言

本年度は，離散構造の限界の解明に関して，

(1) 置換族の構成に関する研究;

(2) ネットワークのルーチングに関する研究;

(3) ネットワークのレイアウトに関する研究;

(4) 大規模システムの高信頼化に関する研究,

を中心に研究を行った．個別の研究内容に関しては，第 2 節以降で詳細に述べるが，各テーマ毎の研究の概略は以下の通りである．

置換族の構成に関する研究

これまでに k-対独立置換族 $\mathcal{F} \subseteq S_n$ の構成に関しては，特定の $k = 2, 3$ と $n = p^m$ (p: 素数) においてその非自明 (対称群・交代群以外) な構成が知られており，一般の k に関しては，その非自明な構成法は存在しないと予想されている．そこで k-対独立置換族の条件を緩和し ε-近似 k-対独立置換族という概念を導入し，代数的手法を用いてそのサイズの下界を導出し，確率的手法を用いてそのサイズの非構成的上界を導出した．そして，その非構成的上界を下回るサイズの ε-近似 2-対独立置換族 $\mathcal{F} \subseteq S_{p^m-1}$ の構成法と ε-近似 3-対独立置換族 $\mathcal{F} \subseteq S_{p^m}$ の構成法を提案した．さらに，Feistel 変換を用いて，任意の k に対する ε-近似 k-対独立置換族の構成法を提案した．

ネットワークのルーチングに関する研究

QoS アルゴリズムの競合比の解析とマルチキャスト通信の遅延最小化について考察している．QoS アルゴリズムに関する研究では，各種のパケットをその優先度に応じて効率的に転送制御するための複数キュー QoS アルゴリズムに関して検討した．一般に QoS スイッチに到来するパケットを事前に予測することは不可能であるので，QoS アルゴリズムはオンラインアルゴリズムとして定式化される．そして，キューに格納されているパケットを破棄することを許さないパケット破棄不可能モデルに着目し，複数優先度を持つ複数キュー QoS アルゴリズムの競合比の解析を行ない，これまで未解明であった非自明な下界を導出するとともに，単一優先度における競合比の下界を改善した．また，マルチキャスト通信について考察し，マルチキャスト木のコスト制限下で遅延を最小化する問題に対する完全多項式時間近似スキームを提案した．

ネットワークのレイアウトに関する研究

グラフの直交描画と 3 次元チャネル配線について考察している．グラフの直交描画に関する研究では，外平面グラフと直並列グラフに対して，少ないベンドを用いて二次元及び三次元に直交描画する多項式時間アルゴリズムを提案した．また，三次元チャネル配線に関する研究では，二端子ネットの組を配線するために必要な三次元チャネルの層数の上界と下界を明らかにした．

大規模システムの高信頼化に関する研究

逐次故障診断と確率的耐故障ネットワークについて考察している．並列計算システムの逐次故障診断に関する研究では，様々なシステムの逐次診断可能次数の上界と下界を統一的な手法を用いて示した．また，確率的耐故障ネットワークに関する研究では，様々なネットワークに対して，疎な確

率的耐故障ネットワークを構成する統一的な手法を提案した.

2 置換族の構成に関する研究

任意の整数 $a \le b$ に対して $[a,b] = \{a,\ldots,b\}$ とし，任意の整数 $n \ge 1$ に対して S_n を集合 $[0,n-1]$ 上の置換全体とする．また，任意の整数 $n \ge k \ge 1$ に対して $[n]_k = n(n-1)\cdots(n-k+1)$ とする．このとき置換族 $\mathcal{F} \subseteq S_n$ が "ε-近似 k-対独立" であるとは，任意の k 個の異なる $x_1, x_2, \ldots, x_k \in [0,n-1]$ と任意の k 個の異なる $y_1, y_2, \ldots, y_k \in [0,n-1]$ に対して，以下が成り立つことを言う.

$$\Pr_{\pi\in\mathcal{F}}\left[\left|\bigwedge_{i=1}^{k}\pi(x_i)=y_i\right] - \frac{1}{[n]_k}\right| \le \frac{\varepsilon}{[n]_k}.$$

特に $\varepsilon = 0$ の場合を "k-対独立" であると言う.

単純な数え上げ論法により，任意の k-対独立置換族 $\mathcal{F} \subseteq S_n$ に対して $|\mathcal{F}| \ge [n]_k$ が成り立つことが示される．一方，これまでに $k = 2$ の場合，任意の $n = p^m$ (p: 素数) に対して $|\mathcal{G}_2| = [n]_2$ となるような 2-対独立置換族 $\mathcal{G}_2 \subseteq S_{p^m}$ の構成法が知られている．具体的には

$$\mathcal{G}_2 = \big\{\pi_{a,b} : \pi_{a,b}(x) = ax+b, \quad a \in \mathbf{GF}(p^m) - \{0\}, b \in \mathbf{GF}(p^m)\big\}.$$

同様に $k = 3$ の場合，任意の $n = p^m + 1$ (p: 素数) に対して $|\mathcal{G}_3| = [n]_3$ となる 3-対独立置換族 $\mathcal{G}_3 \subseteq S_{p^m+1}$ の構成法が知られている．任意の $a,b,c,d \in \mathbf{GF}(p^m)$ に対して $A = \binom{ab}{cd}$ とすると，

$$\mathcal{G}_3 = \begin{cases} \big\{\pi_A : \pi_A(x) = \frac{ax+b}{cx+d}, \quad ad-bc = 1\big\} & p = 2; \\ \big\{\pi_A : \pi_A(x) = \frac{ax+b}{cx+d}, \quad ad-bc \in \{1,e\}\big\} & p \ne 2. \end{cases}$$

ただし $e \in \mathbf{GF}(p^m)$ は任意に固定された平方非剰余であり，任意の $x \in \mathbf{GF}(p^m) \cup \{\infty\}$ に対して，

$$c = 0: \quad \pi_A(x) = \begin{cases} \frac{ax+b}{d} & x \ne \infty; \\ \infty & x = \infty; \end{cases}$$

$$c \ne 0: \quad \pi_A(x) = \begin{cases} \frac{ax+b}{cx+d} & x \notin \{-dc^{-1}, \infty\}; \\ \infty & x = -dc^{-1}; \\ ac^{-1} & x = \infty. \end{cases}$$

2.1 ε-近似 k-対独立置換族の構成 [I]

学術論文 1 において ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ のサイズの下界と非構成的上界を導出し，さらにその非構成的上界を下回る ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ の具体的な構成法を提案した.

まず始めに，代数的手法を用いて，以下のような ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ のサイズの下界 [学術論文 1, Theorem 3.1] を導出した.

定理 1 任意の実数 $\varepsilon \ge 0$ と任意の整数 $n \ge k \ge 1$ に対して，置換族 $\mathcal{F} \subseteq S_n$ が ε-近似 k-対独立であるならば，以下が成り立つ.

$$|\mathcal{F}| \ge \begin{cases} n(n-1)\cdots(n-k+1) & \varepsilon < 1; \\ \dfrac{n(n-1)\cdots(n-k+1)}{1+\varepsilon} & \varepsilon \ge 1. \end{cases}$$

一般的に $\varepsilon \ge 1$ に対して，この下界はこれ以上改善することはできない．実際，第 2 節の冒頭で定義した置換族 $\mathcal{G}_2 \subseteq S_{p^m}$ と $\mathcal{G}_3 \subseteq S_{p^m+1}$ に対して，

$$\begin{aligned} \mathcal{G}_2' &= \big\{\pi \in \mathcal{G}_2 : |\mathcal{G}_2'| = |\mathcal{G}_2|/2\big\} \subseteq \mathcal{G}_2; \\ \mathcal{G}_3' &= \big\{\pi \in \mathcal{G}_3 : |\mathcal{G}_3'| = |\mathcal{G}_3|/2\big\} \subseteq \mathcal{G}_3. \end{aligned}$$

とすると $\varepsilon = 1$ において

$$\begin{aligned} |\mathcal{G}_2'| &= p^m(p^m-1)/2; \\ |\mathcal{G}_3'| &= (p^m+1)p^m(p^m-1)/2, \end{aligned}$$

となり，それぞれ定理 1 の等号を満たす.

次に，確率的手法を用いて，以下のような ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ のサイズの非構成的上界 [学術論文 1, Theorem 3.2] を導出した.

定理 2 任意の実数 $0 < \varepsilon < 1$ と任意の整数 $n \ge k \ge 1$ に対して，以下を満たす ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ が存在する.

$$|\mathcal{F}| = O\left(\frac{k\ln n}{\varepsilon^2}[n]_k\right).$$

さらに，定理 1 および定理 2 より，任意の $\varepsilon > 0$ に対して，コンパクトで多項式時間標本可能な ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ の構成法を提案した.

定理 3 任意の実数 $\varepsilon > 0$ と任意の整数 $n = p^m - 1 \ge \lceil\gamma/\varepsilon\rceil$ (p: 素数) に対して

$$|\mathcal{F}| = \left\lceil\frac{\gamma}{\varepsilon}\right\rceil(1+o(1))[n]_2$$

を満たす多項式時間標本可能な ε-近似 2-対独立置換族 $\mathcal{F} \subseteq S_n$ が構成可能である．ただし，

$$\gamma = \begin{cases} 4 & x^2-x+1 \text{ が } \mathbf{GF}(p^m) \text{ 上で既約;} \\ 6 & x^2-x+1 \text{ が } \mathbf{GF}(p^m) \text{ 上で可約.} \end{cases}$$

証明 (概略): 2-対独立置換族 $\mathcal{G}_2 \subseteq S_{p^m}$ から，以下の手順で置換族 $\mathcal{F} \subseteq S_{p^m-1}$ を構成する．

(1) 交換操作 Swap により置換族 $\mathcal{H}_2 \subseteq S_{p^m-1}$ を生成する．ただし $\mathcal{H}_2 = \mathsf{Swap}(\mathcal{G}_2)$.

(2) シフト操作 Shift_i により置換族 $\mathcal{H}_2^i \subseteq S_{p^m-1}$ を生成する．ただし $\mathcal{H}_2^i = \mathsf{Shift}_i(\mathcal{H}_2)$.

(3) $\mathcal{F} = \mathcal{H}_2^1 \cup \mathcal{H}_2^2 \cup \cdots \cup \mathcal{H}_2^\ell \subseteq S_{p^m-1}$.

交換操作 $\mathsf{Swap} : S_{p^m} \to S_{p^m-1}$ は以下のように定義される: 任意の $\pi \in S_{p^m}$ に対して $\widetilde{\pi} = \mathsf{Swap}(\pi)$ とし，任意の $x \in \mathbf{GF}(p^m) - \{0\}$ に対して

$$\widetilde{\pi}(x) = \begin{cases} \pi(x) & \pi(x) \neq 0; \\ \pi^2(x) = \pi(0) & \pi(x) = 0, \end{cases}$$

とし $\mathcal{H}_2 = \{\widetilde{\pi} = \mathsf{Swap}(\pi) : \pi \in \mathcal{G}_2\} = \mathsf{Swap}(\mathcal{G}_2)$ とする．また，シフト操作 $\mathsf{Shift}_i : S_{p^m-1} \to S_{p^m-1}$ は以下のように定義される: まず始めに，異なる ℓ 個の $\alpha_1, \alpha_2, \ldots, \alpha_\ell \in \mathbf{GF}(p^m) - \{0\}$ を任意に固定．ここで任意の $x \in \mathbf{GF}(p^m) - \{0\}$ に対して，

$$\mathsf{Shift}_i(x) = \begin{cases} (x+\alpha_i)^{-1} & x \neq -\alpha_i; \\ \alpha_i^{-1} & x = -\alpha_i, \end{cases}$$

とし $\mathcal{H}_2^i = \{\sigma : \sigma = \widetilde{\pi} \circ \mathsf{Shift}_i, \widetilde{\pi} \in \mathcal{H}_2\}$ とする．

このとき置換族 $\mathcal{F} \subseteq S_{p^m-1}$ に関して以下が成り立つ [学術論文 1, Lemma 4.6].

補題 1 任意の異なる $x_0, x_1 \in \mathbf{GF}(p^m) - \{0\}$ と任意の異なる $y_0, y_1 \in \mathbf{GF}(p^m) - \{0\}$ に対して，

(a) $\sigma(x_0) = y_0, \sigma(x_1) = y_1$ を満たす置換 $\sigma \in \mathcal{F}$ が少なくとも ℓ 個存在する．

(b) x^2-x+1 が $\mathbf{GF}(p^m)$ 上で既約であるならば，$\sigma(x_0) = y_0, \sigma(x_1) = y_1$ を満たす置換 $\sigma \in \mathcal{F}$ が高々 $\ell+4$ 個存在する．

(c) x^2-x+1 が $\mathbf{GF}(p^m)$ 上で可約であるならば，$\sigma(x_0) = y_0, \sigma(x_1) = y_1$ を満たす置換 $\sigma \in \mathcal{F}$ が高々 $\ell+6$ 個存在する．

補題 1 より定理 3 が容易に導かれる．簡単のため $n = p^m$ とする．ここで x^2-x+1 が $\mathbf{GF}(p^m)$ 上で既約であるとき $\ell = \lceil 4/\varepsilon \rceil$ とする．このとき，補題 1 の (a) 及び (b) より，

$$\left| \Pr_{\sigma \in \mathcal{F}} [\sigma(x_0) = y_0, \sigma(x_1) = y_1] - \frac{1}{n(n-1)} \right| \leq \frac{\varepsilon}{n(n-1)}$$

が成り立つことが導かれる．一方 x^2-x+1 が $\mathbf{GF}(p^m)$ 上で可約であるとき $\ell = \lceil 6/\varepsilon \rceil$ とする．このとき，補題 1 の (a) 及び (c) より，

$$\left| \Pr_{\sigma \in \mathcal{F}} [\sigma(x_0) = y_0, \sigma(x_1) = y_1] - \frac{1}{n(n-1)} \right| \leq \frac{\varepsilon}{n(n-1)}$$

が成り立つことが導かれる． ■

定理 4 任意の実数 $\varepsilon > 0$ と任意の整数 $n = p^m \geq \lceil \gamma/\varepsilon \rceil$ (p: 素数) に対して

$$|\mathcal{F}| = \left\lceil \frac{\gamma}{\varepsilon} \right\rceil (1+o(1))[n]_3$$

を満たす多項式時間標本可能な ε-近似 3-対独立置換族 $\mathcal{F} \subseteq S_n$ が構成可能である．ただし，

$$\gamma = \begin{cases} 6 & x^2+x+1 \text{ が } \mathbf{GF}(p^m) \text{ 上で既約;} \\ 12 & x^2+x+1 \text{ が } \mathbf{GF}(p^m) \text{ 上で可約.} \end{cases}$$

証明 (概略): 3-対独立置換族 $\mathcal{G}_3 \subseteq S_{p^m+1}$ から，以下の手順で置換族 $\mathcal{F} \subseteq S_{p^m}$ を構成する．

(1) 交換操作 Swap により置換族 $\mathcal{H}_3 \subseteq S_{p^m}$ を生成する．ただし $\mathcal{H}_3 = \mathsf{Swap}(\mathcal{G}_3)$.

(2) シフト操作 Shift_i により置換族 $\mathcal{H}_3^i \subseteq S_{p^m}$ を生成する．ただし $\mathcal{H}_3^i = \mathsf{Shift}_i(\mathcal{H}_3)$.

(3) $\mathcal{F} = \mathcal{H}_3^1 \cup \mathcal{H}_3^2 \cup \cdots \cup \mathcal{H}_3^\ell \subseteq S_{p^m}$.

ここで，交換操作 $\mathsf{Swap} : S_{p^m+1} \to S_{p^m}$ は以下のように定義される: 任意の $\pi \in S_{p^m+1}$ に対して $\widetilde{\pi} = \mathsf{Swap}(\pi)$ とし，任意の $x \in \mathbf{GF}(p^m)$ に対して

$$\widetilde{\pi}(x) = \begin{cases} \pi(x) & \pi(x) \neq \infty; \\ \pi^2(x) = \pi(\infty) & \pi(x) = \infty, \end{cases}$$

とし $\mathcal{H}_3 = \{\widetilde{\pi} = \mathsf{Swap}(\pi) : \pi \in \mathcal{G}_3\} = \mathsf{Swap}(\mathcal{G}_3)$ とする．また，シフト操作 $\mathsf{Shift}_i : S_{p^m} \to S_{p^m}$ は

以下のように定義される: まず始めに，異なる ℓ 個の $\alpha_1, \alpha_2, \ldots, \alpha_\ell \in \mathbf{GF}(p^m)$ を任意に固定．ここで任意の $x \in \mathbf{GF}(p^m)$ に対して，

$$\mathsf{Shift}_i(x) = \begin{cases} (x+\alpha_i)^{-1} & x \neq -\alpha_i; \\ 0 & x = -\alpha_i, \end{cases}$$

とし $\mathcal{H}_3^i = \{\sigma : \sigma = \widetilde{\pi} \circ \mathsf{Shift}_i, \widetilde{\pi} \in \mathcal{H}_3\}$ とする．

このとき置換族 $\mathcal{F} \subseteq S_{p^m}$ に関して以下が成り立つ [学術論文 1, Lemma 5.6].

補題 2 任意の異なる $x_0, x_1, x_2 \in \mathbf{GF}(p^m)$ と任意の異なる $y_0, y_1, y_2 \in \mathbf{GF}(p^m)$ に対して，

(a) $\sigma(x_0) = y_0, \sigma(x_1) = y_1, \sigma(x_2) = y_2$ を満たす置換 $\sigma \in \mathcal{F}$ が少なくとも ℓ 個存在する．

(b) $x^2 + x + 1$ が $\mathbf{GF}(p^m)$ 上で既約であるならば，$\sigma(x_0) = y_0, \sigma(x_1) = y_1, \sigma(x_2) = y_2$ を満たす置換 $\sigma \in \mathcal{F}$ が高々 $\ell + 6$ 個存在する．

(c) $x^2 + x + 1$ が $\mathbf{GF}(p^m)$ 上で可約であるならば，$\sigma(x_0) = y_0, \sigma(x_1) = y_1, \sigma(x_2) = y_2$ を満たす置換 $\sigma \in \mathcal{F}$ が高々 $\ell + 12$ 個存在する．

補題 2 より定理 4 が容易に導かれる．簡単のため $n = p^m$ とする．ここで $x^2 + x + 1$ が $\mathbf{GF}(p^m)$ 上で既約であるとき $\ell = \lceil 6/\varepsilon \rceil$ とする．このとき，補題 2 の (a) 及び (b) より，

$$\left| \Pr_{\sigma \in \mathcal{F}} \left[\bigwedge_{i=0}^{2} \sigma(x_i) = y_i \right] - \frac{1}{[n]_3} \right| \leq \frac{\varepsilon}{[n]_3}$$

が成り立つことが導かれる．一方 $x^2 + x + 1$ が $\mathbf{GF}(p^m)$ 上で可約であるとき $\ell = \lceil 12/\varepsilon \rceil$ とする．このとき，補題 2 の (a) 及び (c) より，

$$\left| \Pr_{\sigma \in \mathcal{F}} \left[\bigwedge_{i=0}^{2} \sigma(x_i) = y_i \right] - \frac{1}{[n]_3} \right| \leq \frac{\varepsilon}{[n]_3}$$

が成り立つことが導かれる． ■

2.2 ε-近似 k-対独立置換族の構成 [II]

研究会等論文 1 において，共通鍵暗号方式 DES (Data Encryption Standard) の設計において本質的な役割を果たすフェイステル変換を繰り返し用いて置換族を構成し，カップリング法を用いて以下が成り立つことを明らかにした．

定理 5 任意の $n = p^{2h}$ (p: 素数; h: 正整数) に対して $k = O(\log n)$ であるならば，

$$|\mathcal{F}| = \left(\frac{n^{k^2}}{\varepsilon^k} \right)^{3+o(1)}$$

を満たす ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ が構成可能である．

これは ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ の非自明 (対称群・交代群以外) な最初の構成法である．さらに，本研究で構成された置換族が $O(\log n)$-領域要素別法本可能であることを示した．

マルコフ連鎖は，有限状態集合 $\mathcal{X}$，$\mathcal{X}$ 上の初期分布 μ_0，遷移確率行列 $P = (p_{xy})$ から構成される．ここで全ての $x \in \mathcal{X}$ に対して，

$$\sum_{y \in \mathcal{X}} p_{xy} = 1$$

が成り立つことに注意する．初期分布 μ_0 からスタートして遷移確率行列 P に従って $t \geq 0$ 回遷移した際の分布を μ_t とすると

$$\mu_t = \mu_{t-1} P = \mu_{t-2} P^2 = \cdots = \mu_0 P^t$$

が明らかに成り立つ．有限状態集合 $\mathcal{X}$ 上の任意の分布 ν_1, ν_2 に対して，その距離 $\mathsf{dist}(\nu_1, \nu_2)$ を

$$\begin{aligned} \mathsf{dist}(\nu_1, \nu_2) &= \|\nu_1 - \nu_2\| \\ &= \frac{1}{2} \cdot \sum_{x \in \mathcal{X}} |\nu_1(x) - \nu_2(x)| \end{aligned}$$

と定義し，遷移確率行列 $P = (p_{xy})$ に対して，

$$\beta = \sum_{y \in \mathcal{X}} \min_{x \in \mathcal{X}} p_{xy}$$

を定義する．また $\pi P = \pi$ を満たす有限状態集合 $\mathcal{X}$ 上の分布 pi を定常分布と呼ぶ．このとき以下が成り立つことが知られている．

補題 3 任意の初期分布 μ_0 と任意の $t \geq 0$ に対して，以下が成り立つ．

$$\mathsf{dist}(\mu_t, \pi) = \|\mu_t - \pi\| \leq (1 - \beta)^t.$$

以下では G_+ は加法群を表すものとする．このとき，任意の関数 $g : G_+ \to G_+$ に関する Feistel 変換 $h_g : G_+ \times G_+ \to G_+ \times G_+$ は以下にように定義される: 任意の $(\ell, r) \in G_+ \times G_+$ に対して

$$h_g((\ell, r)) = (r, \ell + g(r)).$$

ここで任意の関数 $g : G_+ \to G_+$ に関して Feistel 変換 h_g は $G_+ \times G_+$ 上の置換となる．従って，任意の関数族 $\mathcal{G} = \{g : G_+ \to G_+\}$ から Feistel 変換によって誘導される置換族 $\mathcal{H}_\mathcal{G} = \{h_g : g \in \mathcal{G}\} \subseteq S_{G_+ \times G_+}$ が自然に定義される．

任意の $k \geq 1$ に対して DIST_k を異なる k 個の二項組 (ℓ_1, r_1), カップリング法を用いて $(\ell_2, r_2), \ldots, (\ell_k, r_k) \in G_+ \times G_+$ 全体と定義すると，Feistel 変換は有限状態集合 DIST_k 上のマルコフ連鎖となる．そこで k-対独立関数族 $\mathcal{G}$ から Feistel 変換によって誘導される置換族 $\mathcal{H}_\mathcal{G} \subseteq S_{G_+ \times G_+}$ と有限状態集合 DIST_k 上の遷移確率行列 Q が自然に定義される．ここで $P = Q^3$ とすると，行列 $P = (p_{xy})$ は k-対独立関数族 $\mathcal{G}$ から 3 回の Feistel 変換によって誘導される有限状態集合 DIST_k 上の遷移確率行列となる．

このとき有限状態集合 DIST_k 上の遷移確率行列 $P = (p_{xy})$ に関して以下が成り立つ [研究会等論文 1, Lemma 3.1].

補題 4 $|G_+| \geq 2\binom{k}{2}$ ならば DIST_k 上の遷移確率行列 $P = (p_{xy})$ に関して以下が成り立つ．

$$\beta = \sum_{y \in \mathsf{DIST}_k} \min_{x \in \mathsf{DIST}_k} p_{xy} \geq 1 - \frac{1}{|G_+|} \cdot \binom{k}{2}.$$

ここで k-対独立関数族 $\mathcal{G}$ から $d = 3e$ 回の Feistel 変換によって誘導される置換族を $\mathcal{H}^e_\mathcal{G} \subseteq S_{G_+ \times G_+}$ とする．このとき，補題 3 と補題 4 より以下の補題 [研究会等論文 1, Theorem 4.1] が導かれる．

補題 5 任意の $0 < \varepsilon < 1$ に対して $d = 3e^*$ とすると，置換族 $\mathcal{H}^{e^*}_\mathcal{G} \subseteq S_{G_+ \times G_+}$ は ε-近似 k-対独立となる．ただし $|G_+| = m, n = m^2$ に関して

$$e^* = \left\lceil \frac{\log[n]_k + \log(1/\varepsilon)}{\log(m/2) - \log\binom{k}{2}} \right\rceil.$$

定理 5 の略証: 任意の素数 p と正整数 h に対して $q = p^h$ とし $G_+ = \mathbf{F}_q$ とする．ここで任意の整数 $k \geq 1$ に対して，以下を定義する．

$$\mathbf{F}_q^{k-1}[x] = \left\{ f : f(x) = \sum_{i=0}^{k} a_i x^i, a_i \in \mathbf{F}_q \right\}.$$

このとき関数族 $\mathbf{F}_q^{k-1}[x] : \mathbf{F}_q \to \mathbf{F}_q$ は k-対独立となる．仮定より $k = O(\log n)$ であるので $m = |\mathbf{F}_q^{k-1}[x]| = q^k$; $\log(m/2) - \log\binom{k}{2} = (1/2 - o(1)) \cdot \log n$ となることに注意すると，

$$\begin{aligned} 3e^* &= 3\left\lceil \frac{\log[n]_k + \log(1/\varepsilon)}{\log(m/2) - \log\binom{k}{2}} \right\rceil \\ &\leq 3\left\lceil \frac{\log n^k + \log(1/\varepsilon)}{\log(m/2) - \log\binom{k}{2}} \right\rceil \\ &= (6 + o(1))k + (6 + o(1)) \cdot \frac{\log(1/\varepsilon)}{\log n} \end{aligned}$$

が成り立つ．ここで $\mathcal{F} = \mathcal{H}^{e^*}_{\mathbf{F}_q^{k-1}[x]}$ とすると

$$|\mathcal{F}| = \left(\frac{n^{k^2}}{\varepsilon^k}\right)^{3+o(1)}.$$

ただし $n = p^{2h}$ (p: 素数; h: 正整数). ■

3 ネットワークのルーチングに関する研究

3.1 QoS アルゴリズムの競合比の解析

近年のインターネットの爆発的な普及に伴い，ネットワーク機器に過剰な負荷がかかり，また帯域損失・パケット消失・応答遅延などの通信品質の劣化が深刻化している．このような通信品質の劣化を防ぐために Quality of Service (QoS) の概念が注目されている．一般に QoS スイッチは m 個のキューを持ち，各キューは到来するパケットを格納するための B 個のスロットを有する．また各パケットはその優先順位を表す “優先度” が割り当てられている．ネットワーク上の通信量はしばしば変化するため，QoS スイッチは転送パケットの優先度の総和を最大にするように到来するパケットの制御を行う．ここで QoS スイッチは，将来到来するパケットの情報を得ることが不可能であるので QoS アルゴリズムはオンラインアルゴリズムとして定式化され，その効率は競合比によって評価される．QoS アルゴリズム ALG が c-競合的であるとは，全てのパケット列 σ に対して

$$\frac{\mathrm{OPT}(\sigma)}{\mathrm{ALG}(\sigma)} \leq c$$

が成り立つことを言う．ただし $\mathrm{ALG}(\sigma)$ はパケット列 σ に対して QoS アルゴリズム ALG が転送し

たパケットの優先度の総和を表すものとし，一方 $\textsc{Opt}(\sigma)$ は，パケット列 σ に対して最適なオフラインアルゴリズム Opt が転送したパケットの優先度の総和を表すものとする．

本研究では，優先度が 1 と $\alpha \geq 1$ に制限された決定性 QoS 問題に関して，その競合比の下界の解析を行い，以下の結果 [学術論文 4] を導出した．

定理 6 任意の QoS アルゴリズム Alg と任意の $\alpha \geq 1$ に対して，パケット列 σ が存在し，

$$\frac{\textsc{Opt}(\sigma)}{\textsc{Alg}(\sigma)} \geq \begin{cases} 1 + \frac{1}{\alpha \ln\left(\frac{\alpha}{\alpha-1}\right)} - \Theta\left(\frac{1}{\min\{m,B\}}\right) \\ \qquad\qquad \alpha \geq \alpha^*; \\ \frac{1}{1-e^{-\tau_0}} - \Theta\left(\frac{1}{\min\{m,B\}}\right) \\ \qquad\qquad 1 \leq \alpha < \alpha^*. \end{cases}$$

ただし τ_0 は $e^{-\tau}(1/\alpha + \tau) = 1 - e^{-\tau}$ の根である．

またこの結果より，単一優先度決定性 QoS 問題に関して，その競合比の下界が 1.466 以上となることが容易に導出される．これは単一優先度決定性 QoS 問題の競合比に関する既知の下界 1.366 を改善するものである．

3.2 マルチキャスト木の構成

マルチキャスト通信において，1 つの送信元と複数の受信先を張るスタイナー木をマルチキャスト木という．マルチキャスト木のリンクの通信コストの総和をそのマルチキャスト木の通信コストという．また，マルチキャスト木上の送信元から各受信先へのパスのリンクの通信遅延の総和の最大値をそのマルチキャスト木の通信遅延という．マルチキャスト通信においては，通信コストと通信遅延を共に最小化するマルチキャスト木を求める問題が基本的である．

これに関して，通信遅延を制限したときに通信コストを最小化するマルチキャスト木を求める問題が従来から活発に研究されている．この問題は，直並列ネットワークに対してさえも，$\mathcal{NP}$ 困難であることが知られており，多くのヒューリスティックアルゴリズムが提案されているが，多項式時間近似アルゴリズムとしては，受信先の数が定数であるという非常に限定された場合に完全多項式時間近似スキームが知られているのみである．本研究では，直並列ネットワークに対して，この問題を解く擬似多項式時間アルゴリズムを初めて提案している．直並列ネットワークに対してこの問題を解く多項式時間近似アルゴリズムが存在するか否かを解明することは今後の課題である．

また，本研究では，通信コストを制限したときに通信遅延を最小化するマルチキャスト木を求める問題について考察している．この問題も直並列ネットワークに対してさえも $\mathcal{NP}$ 困難であることを明らかにすると共に，直並列ネットワークに対して，この問題を解く完全多項式時間近似スキームを提案している．より広いクラスのネットワークに対して多項式時間近似アルゴリズムが存在するか否かを解明することは今後の課題である．

4 ネットワークのレイアウトに関する研究

本研究では，グラフの直交描画と三次元チャネル配線について考察している．

4.1 グラフの直交描画

グラフの辺を座標軸に平行な直線分の系列で描画し，異なる辺の描画が端点以外で交差しないとき，これをそのグラフの直交描画であるという．グラフの直交描画は集積回路の設計などに幅広い応用があり，従来から活発に研究されている．特に，グラフをベンドなしで 2 次元あるいは 3 次元空間に直交描画できるか否かを判定する問題は $\mathcal{NP}$ 完全であることが知られている．また，

(1) 最大次数が高々4 の平面的グラフは，八面体を除外して，各辺に対するベンド数が高々2 で 2 次元直交描画できること;

(2) 最大次数が高々3 の平面的グラフは，4 点完全グラフを除外して，各辺に対するベンド数が高々1 で 2 次元直交描画できること;

(3) 最大次数が高々6 の任意のグラフは各辺に対するベンド数が高々3 で 3 次元直交描画できること，

などが知られている．本研究では，特別な平面的グラフである外平面的グラフと直並列グラフに対

して，少ないベンドを用いて 2 次元及び 3 次元空間に直交描画する多項式時間アルゴリズムを提案している．

外平面的グラフの直交描画に関する研究では，まず最大次数が高々3 で三角形を含まない外平面的グラフはベンドなしで 2 次元直交描画できることを明らかにしている．ベンドなしでは 2 次元直交描画できないような，最大次数が 4 で三角形を含まない外平面的グラフが存在するので，この結果は限界的であることが分かる．また，本研究では，最大次数が高々6 で三角形を含まない外平面的グラフはベンドなしで 3 次元直交描画できることも示している．

直並列グラフの直交描画に関する研究では，まず最大次数が高々4 の任意の直並列グラフは各辺に対するベンド数が高々1 で 2 次元直交描画できることを明らかにしている．ベンドなしでは 2 次元直交描画できないような，最大次数が高々4 の直並列グラフが存在するので，この結果は限界的であることが分かる．また，本研究では，最大次数が高々6 の任意の直並列グラフは各辺に対するベンド数が高々2 で 3 次元直交描画できることを明らかにしている．最大次数が高々6 の任意の直並列グラフが各辺に対するベンド数が高々1 で 3 次元直交描画できるか否かを明らかにすることは今後の課題である．

4.2 3 次元チャネル配線

3 次元チャネル配線は 3 次元集積回路設計における基本的な問題の一つであり，いくつかの先駆的研究が散見されるが，いずれも本質的には 2 次元あるいは 2.5 次元のチャネル配線モデルであり，本来の 3 次元チャネル配線のモデルは見当たらない．

そこで本研究では，初めて自然で一般的な 3 次元チャネル配線の以下のようなモデルを提案している．一対の平行な境界面上に端子が配置されている 3 次元格子グラフを 3 次元チャネルという．同一ネットの端子を木で連結し，異なるネットに対する木が点非共有であるとき，これを 3 次元チャネル配線という．3 次元チャネル配線においては，端子が配置されている一対の平行な境界面の間の距離 (これを 3 次元チャネルの高さという) を最小化する問題が基本的である．

また，本研究では，このモデルの下で与えられた 2 端子ネットの組を配線するために必要な 3 次元チャネルの高さの上界と下界を明らかにしている．特に，n 個の 2 端子ネットは高さ $O(\sqrt{n})$ の 3 次元チャネル内で長さ $O(\sqrt{n})$ の配線を用いて配線できることを明らかにすると共に．配線するためには高さ $\Omega(\sqrt{n})$ の 3 次元チャネルを必要とするような n 個の 2 端子ネットの組が存在することを示している．与えられた 2 端子ネットの組を配線するために必要な 3 次元チャネルの高さを最小化する問題の計算複雑度の解明と実際的な配線アルゴリズムの設計は今後の課題である．

5 大規模システムの高信頼化に関する研究

本研究では，並列計算システムの逐次故障診断と確率的耐故障ネットワークについて考察している．

5.1 並列計算システムの逐次故障診断

並列計算システムの故障診断の研究には長い歴史があるが，一度にすべての故障ユニットを同定する同時診断と一度に 1 つの故障ユニットを同定する逐次診断に分類して活発に研究されている．従来から，同時診断可能性に関するシステムの特徴付けはよく知られているが，逐次診断可能性に関するシステムの特徴付けについては知られていない．そこで本研究では，様々なシステムの逐次診断可能次数の上界と下界を統一的な手法を用いて示している．特に，逐次診断可能次数の非自明な上界は初めて示されたものであり，注目を集めている．

より詳細には，まず新しい自然な逐次診断アルゴリズムを提案し，N 個のプロセッサから成る任意のシステムの逐次診断可能次数が少なくとも $\Omega(\sqrt{N})$ であることを明らかにしている．また，非常に一般的な統一的手法を用いて，N 点から成る d 次元グリッドは逐次 $O(N^{d/(d+1)})$ 診断可能であること，及び N 点から成る k 分木は $O(\sqrt{kN})$ 診断可能であることを示している．さらに，N 点から成るハイパーキューブの逐次診断可能次数は少なくとも $\Omega(N/\sqrt{\log N})$ であり，多く

とも $O(N \log\log N/\sqrt{\log N})$ であることを明らかにすると共に，N 点から成る CCC, シャッフル交換グラフ，及び deBruijn グラフの逐次診断可能次数は $\Theta(N/\log N)$ であることを示している．この統一的な手法を用いて，逐次診断可能性に関するシステムの特徴付けを与えることは今後の課題である．

5.2 確率的耐故障ネットワーク

ネットワーク G^* は，定確率で独立にプロセッサが故障しても正常なプロセッサから成るネットワーク G を高い確率で含んでいるとき，G の確率的耐故障ネットワークであるという．この概念は参考文献 [1] で提案され，様々な考察がなされている．特に，N 個のプロセッサと M 本の通信リンクから成る任意のネットワークに対して，$O(N)$ 個のプロセッサと $O(M \log^2 N)$ 本の通信リンクから成る確率的耐故障ネットワークが存在することを明らかにすると共に，$O(N)$ 個のプロセッサと $o(M \log^2 N)$ 本の通信リンクから成る確率的耐故障ネットワークが存在するか否かという興味深い公開問題を提案している．

本研究では，様々な実際的なネットワークに対して，この公開問題を肯定的に解決している．すなわち，確率的故障ネットワークを構成する統一的な手法を提案し，N 個のプロセッサと M 本の通信リンクから成る Cayley, deBruijn, シャッフル交換, 及び部分 k 木などのネットワークに対しては，$O(N)$ 個のプロセッサと $O(M \log N)$ 本の通信リンクから成る確率的耐故障ネットワークが存在することを明らかにしている．ここで，Cayley ネットワークは circulant, ハイパーキューブ, CCC, バタフライ, 星, 及びパンケーキなどのよく知られている多くのネットワークを含んでいることに注意されたい．この統一的な手法を用いて，N 個のプロセッサと M 本の通信リンクから成る任意のネットワークに対して，$O(N)$ 個のプロセッサと $O(M \log N)$ 本の通信リンクから成る確率的耐故障ネットワークを構成することができるか否かを明らかにすることは，興味深い今後の課題である．

本研究では，さらに閉路ネットワークの確率的耐故障ネットワークについても考察している．参考文献 [1] において，N 個のプロセッサから成る閉路ネットワークに対して，$O(N)$ 個のプロセッサと $O(N)$ 本の通信リンクから成る確率的耐故障ネットワークが存在することが述べられているが，その証明には不備があり，不完全なものであった．そこで本研究では，この不備を補い，完全な証明を与えると共に，この証明で構成している確率的耐故障ネットワークは極めて実際的であることを計算機実験により明らかにしている．

6 結論

以上述べたように，本年度は，離散構造に関して，

(1) 置換族の構成 (近似的 k-独立置換族の構成);

(2) ネットワークのルーチング (QoS アルゴリズム・マルチキャスト木の構成);

(3) ネットワークのレイアウト (グラフの直交描画・3 次元チャネル配線);

(4) 大規模システムの高信頼化 (並列計算システムの逐次故障診断・確率的耐故障ネットワーク),

を中心に研究を行った．次年度は，代数的および確率的手法を駆使して，今年度成果をより発展させていく計画である．

参考文献

[1] P. Fraigniaud, C. Kenyon, A. Pelc, Finding a target subnetwork in sparse networks with random faults, Inform. Process. Lett. 48 (1993) 297-303.

研究業績一覧

著書

1. 上野修一，高橋篤司:
“情報とアルゴリズム（電子情報通信工学シリーズ）”, 森北出版株式会社,（刊行予定）.
概要: グラフ理論，アルゴリズム理論，及び計算複雑度の理論の入門書である．

学術論文

1. T. Itoh, Y. Takei, and J. Tarui:
"Constructing Families of ε-Approximate k-Wise Independent Permutations", IEICE Trans. on Fundamentals, Vol.E87-A, pp.993-1003, 2004.
概要: The notion of k-wise independent permutations has several applications. From the practical point of view, it often suffices to consider almost (i.e., ε-approximate) k-wise independent permutation families rather than k-wise independent permutation families, however, we know little about how to construct families of ε-approximate k-wise independent permutations of small size. For any $n > 0$, let S_n be the set of all permutations on $\{0, 1, \ldots, n-1\}$. In this paper, we investigate the size of families of ε-approximate k-wise independent permutations and show that (1) for any constant $\varepsilon \geq 0$, if a family $\mathcal{F} \subseteq S_n$ of permutations is ε-approximate k-wise independent, then $|\mathcal{F}| \geq n(n-1)\cdots(n-k+1)$ if $\varepsilon < 1$; $|\mathcal{F}| \geq \{n(n-1)\cdots(n-k+1)\}/(1+\varepsilon)$ otherwise; (2) for any constant $0 < \varepsilon \leq 1$, there exists a family $\mathcal{F} \subseteq S_n$ of ε-approximate k-wise independent permutations such that $|\mathcal{F}| = O(\frac{k \ln n}{\varepsilon^2} n(n-1)\cdots(n-k+1))$; (3) for any constant $\varepsilon > 0$ and any $n = p^m - 1$ with p prime, it is possible to construct a polynomial time samplable family $\mathcal{F} \subseteq S_n$ of ε-approximate pairwise independent permutations such that $|\mathcal{F}| = O(n(n-1)/\varepsilon)$; (4) for any constant $\varepsilon > 0$ and any $n = p^m$ with p prime, it is possible to construct a polynomial time samplable family $\mathcal{F} \subseteq S_n$ of ε-approximate 3-wise independent permutations such that $|\mathcal{F}| = O(n(n-1)(n-2)/\varepsilon)$. Our results are derived by combinatorial arguments, i.e., probabilistic methods and linear algebra methods.

2. T. Yamada, T. Ohtsuka, A. Watanabe, and S. Ueno:
"On sequential diagnosis of multiprocessor systems", Discrete Applied Mathematics, Vol.146, pp.311-342, 2005.
概要: This paper considers the problem of sequential fault diagnosis for various multiprocessor systems. We propose a simple sequential diagnosis algorithm and show that the degree of sequential diagnosability of any system with N processors is at least $\Omega(\sqrt{N})$. We also show upper bounds for various networks. These are the first nontrivial upper bounds for the degree of sequential diagnosability, to the best of our knowledge. Our upper bounds are proved in a unified manner, which is based on the very definition of sequential diagnosability. We show that a d-dimensional grid and torus with N vertices are sequentially $O(N^{d/(d+1)})$-diagnosable, and an N-vertex k-ary tree is $O(\sqrt{kN})$-diagnosable. Moreover, we prove that the degree of sequential diagnosability of an N-vertex hypercube is at least $\Omega(N/\sqrt{\log N})$ and at most $O(N \log\log N/\sqrt{\log N})$, and those of an N-vertex CCC, shuffle-exchange graph, and de Bruijn graph are $\Theta(N/\log N)$.

3. S. Tayu, T. Ghazi Al-Mutairi, and S. Ueno:
"Cost-Constrained Minimum-Delay Multicasting", Lecture Notes in Computer Science, vol.3381, pp.330-339, 2005.
概要: We consider a problem of cost-constrained minimum-delay multicasting in a network, which is to find a Steiner tree spanning the source and destination nodes such that the maximum total delay along a path from the source node to a destination node is minimized, while the sum of link costs in the tree is bounded by a constant. The problem is $\mathcal{NP}$-hard even if the network is series-parallel. We present a fully polynomial time approximation scheme for the problem if the network is series-parallel.

4. T. Itoh and T. Nagumo:
"Improved Lower Bounds for Competitive Ratio of Multi-Queue Switches in QoS Networks", to appear in IEICE Trans. on Fundamentals, 2005.
概要: The recent burst growth of the Internet use overloads networking systems and degrades the quality of communications, e.g., bandwidth loss, packet drops, delay of responses, etc. To overcome such degradation of the communication quality, the notion of Quality of Service (QoS) has received attention in practice. In general, QoS switches have several queues and each queue has several slots to store arriving packets. Since network traffic changes frequently, QoS switches need to control arriving packets to maximize the total priorities of transmitted packets, where the priorities are given by nonnegative values and correspond to the quality of service required for each packet. In this paper, we derive lower bounds for the competitive ratio of deterministic multi-queue nonpreemptive QoS problem of priorities 1 and $\alpha \geq 1$: $1+/\alpha \ln(\frac{\alpha}{\alpha-1})$ if $\alpha \geq \alpha^*$; $1/(1-e^{-\tau_0})$ if $1 \leq \alpha < \alpha^*$, where $\alpha^* \approx 1.657$ and τ_0 is a root of the equality that $e^{-\tau}(1/\alpha+\tau) = 1-e^{\tau}$. As an immediate result, this shows a lower bound 1.466 for the competitive ratio of deterministic multi-queue nonpreemptive QoS problem of single priority, which slightly improves the best known lower bound 1.366.

5. K. Nomura, S. Tayu, and S. Ueno:
"On the Orthogonal Drawing of Outerplannar Graphs", Lecture Notes in Computer Science, Vol.3106, pp.300-308, 2004.
概要: In this paper we show that an outerplanar graph G with maximum degree at most 3 has a 2-D orthogonal drawing with no bends if and only if G contains no triangles. We also show that an outerplanar graph G with maximum degree at most 6 has a 3-D orthogonal drawing with no bends if and only if G contains no triangles.

6. T. Yamada, K. Nomura, and S. Ueno:
"Sparse networks tolerating random faults", Discrete Applied Mathematics, Vol.137, pp.223-235, 2004.
概要: A network G^* is called random-fault-tolerant (RFT) network for a network G if G^* contains a fault-free isomorphic copy of G with high probability even if each processor fails independently with constant probability. This paper proposes a general method to construct an RFT network G^* for any network G with N processors such that G^* has $O(N)$ processors. Based on the construction, we also show that if G is a Cayley, de Bruijn, shuffle-exchange, or partial k-tree network with N processors and M communication links then we can construct an RFT network for G with O(N) processors and $O(M \log N)$ communication links. Cayley networks contain many popular networks such as circulant, hypercube, CCC, wrapped butterfly, star, and pancake networks.

研究会等

1. T. Itoh, T. Nagatani, and J. Tarui:
"Explicit Construction of k-Wise Nearly Random Permutations by Iterated Feistel Transform", IEICE Technical Report, Vol.COMP2004-7, pp.45-52, 2004.
概要: A notion of k-wise random permutations has several theoretical applications. From the practical point of view, it often suffices to consider ε-approximate k-wise random permutation families rather than k-wise random permutation families, however, we know little about how to construct families of ε-approximate k-wise random permutations of small size. For any integer $n > 0$, we use S_n to denote the set of all permutations on $\{0, 1, \ldots, n-1\}$. In this paper, we iteratively apply the *Feistel Transform* and

show that for any $n = p^{2h}$ with p prime and any $k = O(\log n)$, there exists a family $\mathcal{F} \subseteq S_n$ of ε-approximate k-wise random permutations such that $|\mathcal{F}| = (n^{k^2}/\varepsilon^k)^{3+o(1)}$. This is the first nontrivial construction for families of ε-approximate k-wise random permutations. To capture efficient evaluation of permutation families in practice, we introduce a notion of "$s(n)$-space pointwise samplability" and show that the family $\mathcal{F} \subseteq S_n$ of permutations constructed in this paper is $O(\log n)$-space pointwise samplable.

2. K. Nomura, S. Tayu, and S. Ueno:
"On the Orthogonal Drawing of Series-Parallel Graphs", IPSJ SIG Technical Report, Vol.2004-AL-98, pp.25-32, 2004.
概要: We show in this paper that every series-parallel graph with maximum degree at most 4 has a 1-bend 2-D orthogonal drawing. We also show that every series-parallel graph with maximum degree at most 6 has a 2-bend 3-D orthogonal drawing.

3. S. Tayu, P. Hurtig, Y. Horikawa, and S. Ueno:
"On the Three-Dimensional Channel Routing", IPSJ SIG Technical Report, Vol.2004-AL-98, pp.19-23, 2004.
概要: The 3-D channel routing is a fundamental problem on the physical design of 3-D integrated circuits. The 3-D channel is a 3-D grid G and the terminals are vertices of G located in the top and bottom layers. A net is a set of terminals to be connected. The object of the 3-D channel routing problem is to connect the terminals in each net with a tree (wire) in G using as few layers as possible and as short wires as possible in such a way that wires for distinct nets are disjoint. This paper shows that any set of n 2-terminal nets can be routed in a 3-D channel with $O(\sqrt{n})$ layers using wires of length $O(\sqrt{n})$. We also show that there exists a set of n 2-terminal nets that requires a 3-D channel with $\Omega(\sqrt{n})$ layers to be routed.

4. S. Tayu, T. Ghazi Al-Mutairi, and S. Ueno:
"Cost-Constrained Minimum-Delay Multicasting", Technical Report of IEICE, Vol.104, no.115, pp.43-48, 2004.
概要: We consider a problem of cost-constrained minimum-delay multicasting in a network, which is to find a Steiner tree spanning the source and destination nodes such that the maximum total delay along a path from the source node to a destination node is minimized, while the sum of link costs in the tree is bounded by a constant. The problem is $\mathcal{NP}$-hard even if the network is series-parallel. We present a fully polynomial time approximation scheme for the problem if the network is series-parallel.

学会大会等

1. S. Tayu and S. Ueno:
"A Note on the Three-Dimensional Channel Routing", Proceedings of the 2005 IEICE General Conference, p.30, 2005.

2. K. Inoue, K. Nomura, S. Tayu, and S. Ueno:
"A Note on Sparse Networks Tolerating Random Faults for Cycles", Proceedings of the 2005 IEICE General Conference, p.31, 2005.

3. K. Nomura, S. Tayu, and S. Ueno:
"On the Two-Dimensional Orthogonal Drawing of Series-Parallel Graphs", Proceedings of the 2004 IEICE Society Conference, 2004.

4. S. Tayu, P. Hurtig, Y. Horikawa, and S. Ueno:
"On the Three-Dimensional Channel Routing", Proceedings of the 2004 IEICE Society Conference, 2004.

5. H. Kawakita, T. Yamada, and S. Ueno:
"Efficient VLSI Decompositions for de Brui-

jin Graphs", Proc. of the 66th National Convention of IPSJ, Vol.1, pp.265-266, 2004.

B02: 暗号解析手法の計算量理論による改良とそれに基づく暗号方式

田中 圭介 † 渡辺 治 † 戸田 誠之助 ‡

† 東京工業大学 大学院情報理工学研究科
数理・計算科学専攻
〒 152-8552 東京都目黒区大岡山 2-12-1
{keisuke, watanabe}@is.titech.ac.jp

‡ 日本大学 文理学部 情報システム解析学科
〒 156-8550 東京都世田谷区桜上水 3-25-40
toda@cssa.chs.nihon-u.ac.jp

1 研究の目的と活動の概要

暗号解析手法の計算量理論による改良とそれに基づく暗号方式の提案を行うために，具体的な目標を以下のように三つ定める．これらは独立に存在するわけではなく，おおまかには，目標３が，目標１および２をふまえた最終的な目標となる．また，それぞれの目的における成果は他への研究指針となり互いに密接に関連する．

暗号の安全性に関する精密な解析手法の開発

暗号方式に対する攻撃はある種の計算問題であるとみなすことができる．また，暗号方式のモデルはある種の計算モデルであるとみなすことができる．計算量理論は，これまで多種の計算問題に内在する計算構造を明らかにしてきているが，グラフ同型性判定問題や群に関わる様々な計算問題などに象徴される『計算構造が不明な離散的計算問題』もまた数多く存在する．暗号方式に対する攻撃についても，このような計算構造が不明な離散的計算問題であると考えられる．そこで本研究ではまず，このような計算問題に関して，それらに内在するはずの本質的な計算構造を探究する．また，その解析をもとに，それらの計算問題を様々な計算モデル上で計算する際の限界と可能性を明らかにする．この解析手法を応用し，暗号の安全性に関する精密な解析手法を開発する．

暗号の効率に関する精密な解析手法の開発

暗号方式は安全であるだけでなく効率的に動作する必要がある．また，通常のコンピュータ上での動作だけではなく，携帯電話や IC カードなどのプロセッサの処理スピードが遅い状況やメモリが少ない状況での動作がしばしば要求される．理論的解析については，定数係数は無視してオーダーで議論するのが主流であり，様々な状況における暗号アルゴリズムの効率の詳細な解析は計算機を用いたシミュレーションを行うなど実験的な手法に頼らざるを得なかった．そこで本研究ではまず，細かな尺度で計算コストを測るための手法として，定数係数までも考慮に入れた計算量理論を開発する．この計算量理論を応用し，暗号の効率に関する精密な解析手法を開発する．

目的１および２に基づく具体的暗号方式の提案

暗号プロトコルのうち最も基本的なものとしては公開鍵暗号がある．そこでまず，この公開鍵暗号に対する具体的方式の提案を行う．設計にあたっては目的１および２の考察をふまえて行う．すなわち，暗号の安全性および効率に関する精密な解析手法のもとで優れた暗号方式の提案を目的とする．さらには，公開鍵暗号以外の，電子署名，認証など，他の暗号プロトコルに対する具体的方式の提案も行う．

目的 1 に関しては，戸田が，chordal graph を対象としたグラフ同型性判定問題ならびにグラフ自己同型群計算問題に関する研究を行った．また，この目的 1 に関しては研究集会を 3 月 19 日 (土) に日本大学文理学部において開催し，chordal graph に関する計算問題ならびにアルゴリズムを中心に，研究成果の発表と新たな課題探求に向けた討論を

行った．

目的 2 に関しては，渡辺が，充足可能性問題に対するアルゴリズム，および，計算量クラスの相対化における妥当な比較の枠組に関してそれぞれ研究を行った．

目的 3 に関しては，田中が，公開鍵暗号に関する様々な考察および提案を行った．

2 暗号の安全性に関する精密な解析手法に関する活動概要

2.1 chordal graph を対象としたグラフ同型性判定問題ならびにグラフ自己同型群計算問題

戸田は，chordal graph を対象としたグラフ同型性判定問題ならびにグラフ自己同型群計算問題に関する研究を行った．これらの問題は，いずれも一般のグラフに対する同型性判定問題と同等の計算量を持つことが知られており，このため，その計算量は不明の状況であり，一般的には計算困難であると予想されている．

今年度は，まず，chordal graph の部分クラスの中で同型性判定問題の計算量が不明とされていた chordal bipartite graph と strongly chordal graph に関して，その計算量を明らかにすべく研究を行った．その結果，両方にクラスに対して，その同型性判定問題の計算量が一般のグラフに対する同型性判定問題と同等であることを示すことができた．従来の結果として，interval graph や rooted directed path graph に対して同型性判定問題が多項式時間計算可能であることが示されていた．これらのクラスは strongly chordal graph の部分クラスとなる（換言すれば，strongly chordal graph はそれらのクラスと chordal graph の中間に位置する）ことも知られていたので，本研究の成果によって，chordal graph に対するグラフ同型性判定問題の計算困難性の境界が interval graph や rooted directed path graph と strongly chordal graph の中間に位置することが判明した．同様に，chordal bipartite graph は bipartite graph と interval bigraph の中間に位置し，bipartite graph に対するグラフ同型性判定問題が一般のグラフの同型性判定問題と同等の計算量を持つこと，ならびに，interval bigraph に対する同型性判定問題については多項式時間計算可能であることがすでに知られていたので，本研究によって，chordal graph に対するグラフ同型性判定問題の計算困難性の境界が interval bigraph と chordal bipartite graph の中間に位置することも判明した．

次に，chordal graph の不変量を制限した場合に関して研究を行った．従来，chordal graph のクリーク数を制限した場合には同型性判定問題に関して多項式時間計算可能であることが知られていた．chordal graph における極大クリークの間の隣接関係がクリーク木と呼ばれる木構造によって表現され得ることが知られており，また，chordal graph の構造解析や様々な計算問題の効率的解法の設計のためにクリーク木がよく利用されていることから，クリーク数を制限するという着眼点はごく自然のことと思われる．一方，chordal graph における極大クリークは単体成分と呼ばれるより小さなクリークに（一意的に）分解することができて，しかも単体成分の間の隣接関係もクリーク木と同様の木構造によって表現することができることから，クリーク数を制限するという着眼点は必ずしも本質的ではなく，大きなクリークを有するような chordal graph であっても単体成分のサイズ（頂点数）が小さいときには同型性判定を多項式時間で判定できるのではないかと予想するに至った．例えば，頂点数の 1/3 程度の大きさのクリークを持ちながらも，単体成分の最大サイズが 2 であるような chordal graph（のクラス）を容易に定義することができる．このようなグラフに対して従来の同型性判定アルゴリズムでは指数時間を必要とするが，その時間量は本質的ではなく，実際には多項式時間で同型性を判定できるのではないかと思われた．本研究では，実際に，この予想を証明した．すなわち，各々の単体成分が小さいときには，クリーク数の大小に関わらず，同型性判定問題が多項式時間判定可能であることを示した．

3　暗号の効率に関する精密な解析手法に関する活動概要

3.1　充足可能性問題に対するアルゴリズム

充足可能性問題の様々な形式のものに対する従来のアルゴリズムの効率の改善に向けて，最悪時と平均時の両面からの研究を行なった．

最悪時の計算効率の改善

最悪時の計算効率を改善する研究では，充足可能性問題の中でも最も標準的な 3-SAT 問題を対象とした．この問題は，3-CNF 形式で与えられる命題論理式の充足可能性を判定する（あるいは，充足解を求める）問題である．この問題に対しては，多くの研究者がアルゴリズムの改良を進めてきた．計算過程で乱数を用いる乱択型のアルゴリズムでは，岩間らのグループのアルゴリズムが現在のところ最速で O(1.324**n) の計算時間である．一方，乱数を用いない通常型（決定性）のアルゴリズムは，Schoning らが O(1.481**n) 時間のものを示されている．現在では，Bruggemann と Kern による O(1.473**n) 時間のアルゴリズムが最速である．

本年度，渡辺は，山本（渡辺が指導する博士課程の学生）とともに，決定性のアルゴリズムの改良を試みた．現在までに，山本が，Schoning らのアルゴリズムを（効率を落すことなく）簡略化することに成功しており，現在は，その簡単化されたアルゴリズムに対する改良を行なっている．

平均的にうまく働くアルゴリズムの解析

充足可能性問題に対しては，平均的にうまく働くアルゴリズムがいくつか知られている．中でも局所探索アルゴリズムは，構造が簡単だが，平均的に非常によい効率を出す場合があることが知られている．

渡辺を中心に，こうした局所探索アルゴリズムの平均的な効率を解析する研究が行なわれているが，本年度は，その解析手法の核の 1 つである「疑似平均」の近似度についての解析を中心に行なった．その結果，単純なマルコフ過程においては，平均状態を解析する手法として，この疑似平均が有効であることを厳密に証明することができた．

さらに，その解析手法を活かして，二種類の充足可能問題（パリティ SAT 問題と 3-SAT 問題）に対し，二種類の局所探索アルゴリズム（貪欲型と酔歩型）の違いを明確に示すことができた．さらには，その解析の中から，貪欲型局所探索アルゴリズムの改良も提案することができた．

3.2　計算量クラスの相対化における妥当な比較の枠組

計算量クラスの違いを示すことの難しさを議論する枠組に相対化計算の枠組がある．渡辺は Cai とともに，この相対化計算の枠組について再考する研究を行なっている．これまでの相対化の議論には妥当でない比較が含まれている，というのがその動機である．

具体的には，たとえば P = NP のような等号関係をシミュレーションにより示す際に，これまでの相対化の議論では，シミュレーションする側が，シミュレーションされる側より，より多くのオラクル情報を利用できることを用いてシミュレーションを行なっていた．これでは妥当な比較ができない，と考えたのである．

そこで，妥当な比較をするための制限を導入し，新しい相対化比較の枠組を提案した．今年度は，その枠組のもとで，まず，BPP と PH の比較を行ない，最終的には P = PH となるオラクルを構成することができた．これは P と PH の計算の難しさの差を，標準的な手法では示すことができない，という予測に対する，きわめて強い状況証拠を与えたことになる．また，PH の計算の難しさの特徴付けにもなっている．

4　目的１および２に基づく具体的暗号方式に関する活動概要

田中は具体的暗号方式に関して以下のような様々な考察および提案を行った．

4.1 匿名性をもつ暗号プロトコル

公開鍵秘匿通信において，暗号文をみただけではその受信者が特定できないとき，もしくは，署名において，署名を生成した人が特定できないとき，その公開鍵秘匿通信方式，もしくは署名方式は，匿名性をみたすという．匿名性を達成するような方式を構成するためには，暗号文，または署名の値域を各ユーザーで共通にすることが必要である．本論文では，匿名性を達成するためのテクニックに着目し，RSA ベースの公開鍵秘匿通信，もしくは署名において有効な sampling twice と呼ばれる新たなテクニックを提案した．このテクニックは，$|N| = k$ をみたす任意の N について，$[0, N)$ 上の一様分布を $[0, 2^k)$ 上の一様分布に変換するものである．さらに，sampling twice テクニックを利用して，公開鍵秘匿通信，否認不可署名，指定検証者署名，リング署名を構成した．これらは匿名性を達成しており，さらに暗号文や署名のサイズ，復号や検証のコストに関して効率のよい方式となっている．

さらに，ElGamal 暗号と Cramer-Shoup 暗号をもとにした匿名性を持つ暗号方式も提案した．以前の方式は，ユーザー全員が共通の群を利用しなければ匿名性を達成することができなかった．我々の方式は，それよりも弱い制約の下で，匿名性を達成できる方式である．具体的には，各ユーザーは safe prime を選び，その素数の上での平方剰余群を利用している．ElGamal 暗号をベースにした方式は，選択平文攻撃に対する匿名性と判別不可能性を達成し，Cramer-Shoup 暗号は適応的選択暗号文攻撃に対する匿名性と判別不可能性を達成している．

4.2 特殊な機能をもつ暗号プロトコル

匿名性をもつ暗号プトロコル以外にも特殊な機能をもつ暗号プロトコルを提案した．

まず，Computational Bilinear Diffie-Hellman 問題に基づく複数キーワード検索つき公開鍵暗号方式を提案した．Park, Kim, Lee は複数キーワード検索つき公開鍵暗号方式 (PECK) を提案した．彼らは具体的な方式を 2 つ提案しており，それらは Decisional Bilinear Diffie-Hellman problem の困難性に基づいて安全性が証明されている．我々は彼らの方式を拡張した新たな方式を提案した．この方式は Park らの仮定よりも弱い仮定である Computational Bilinear Diffie-Hellman problem の困難性を仮定することで安全性を証明することができる方式である．

つぎに，Cramer-Shoup の構成法による平方剰余問題と関連する暗号方式を提案した．Eurocrypt '02 において Cramer と Shoup は適応的選択暗号文攻撃に対して安全な公開鍵暗号の一般的構成法を提案した．我々はこの構成法を用いて新たに具体的に適応的選択暗号文攻撃に対し安全な公開鍵暗号を提案した．彼らは安全性が平方剰余判定問題に依存する公開鍵暗号を具体的に提案していたが，この暗号は離散対数問題，n 次剰余判定問題に安全性が基づく暗号よりも効率が悪かった．我々は平方剰余判定問題と関係を持つ問題を提案し，その問題に安全性が基づく公開鍵暗号を提案した．この暗号は Cramer と Shoup が提案した平方剰余判定問題に基づく暗号よりも効率的である．

また，指定検証者署名への変換が可能な Aggregate Signature　も提案した．二人以上の署名を一つにまとめる aggregate signature と呼ばれる署名がある．本論文では，署名の所有者に，任意の指定された検証者への署名を指定させる機能を追加した aggregate signature を提案した．この機能により，指定された検証者以外は署名を検証できないので，他の人の手に渡った署名は，誰もが検証できる形で送信することができない．

さらには，Groth，古川によるプロトコルのような，honest verifier ゼロ知識証明であるシャッフルに対する証明方式を提案した．古川，佐古，Groth や古川によって提案された以前の方式とは異なり，我々の方式は，メッセージの部分に加法準同型性を持つ Paillier の暗号系によって暗号化された要素のシャッフルとして使う事ができる．以前の方式で使われた ElGamal 暗号方式はこの性質は持っていない．

4.3 暗号プロトコルに関するモデルおよび既存方式の安全性

暗号プロトコルに関するモデルおよび既存方式の安全性に関しても以下のような研究を行った．

まず，認証付き鍵交換プロトコルにおける non-

malleability に基づく安全性について考察した．ここでは，パスワードに基づいた認証付き鍵交換 (AKE) プロトコルを扱った．2000 年に Bellare, Pointcheval, Rogaway によって AKE の厳密なモデルが提案された．我々は，セッションキーの non-malleability 性に基づいた AKE の新しい安全性を定義し，次にこの安全性が Bellare, Poincheval, Rogaway によって提案されたものと等価であることを示した．さらに，この新しい安全性を用いて，ランダムオラクルモデルでは安全であるが，衝突困難性に基づくハッシュ関数を用いたモデルでは安全でなくなるプロトコルがあることを示した．

つぎに，ランダムオラクルモデルを用いたプロトコルの指標と方式について考察した．ランダムオラクルモデルの研究では，ランダムオラクルをつかった方式と，ランダムオラクルの部分を，ある関数の集合からランダムに選んだ関数に置き換えた方式との gap に関する研究が注目されている．我々はランダムオラクルモデルにおける方式の研究の異なる方向性を考える．我々は，ランダムオラクルに対する全ての質問と答えを表現するのに必要な表のサイズに注目し，ランダムオラクルモデルでの公開鍵秘匿通信方式や署名方式における表のサイズの減らし方を示した．さらに，この考えを PSS-R と OAEP に応用した方式を提案し，その安全性を証明した．

さらには，中程度の難しさをもつ関数のモデルと方式についても考察した．moderately-hard function は様々なアプリケーションを持ち，関連する論文も数多く発表されている．しかしながら，moderately-hard function の厳密なモデルは提案されていなかった．本論文では，まず moderately-hard function の厳密なモデルを提案する．ここでは，計算モデルを構成し，moderately-hard function に必要とされる性質を調査した．さらに，moderately-hard function として利用できるいくつかの関数を提案した．この関数は，$p^r q$ の素因数分解の困難性と primitive function の連続計算という二つのアイデアに基づいている．

5 グラフアルゴリズムに関するミニ研究集会

戸田と田中が世話役となり，Chordal graph に関する計算問題ならびにアルゴリズムを中心に，研究成果の発表と新たな課題探求に向けた討論を行った．詳細は次の通り．

日時： 3 月 19 日 (土)　午前 10 時 ～ 午後 6 時
場所： 日本大学文理学部 8 号館レクチャーホール
参加者数： 19 名
研究発表：

(1) 10:00~11:20，Computing automorphism groups of chordal graphs whose simplicial components are of small size，戸田誠之助（日大文理）
（概要）小さなサイズの単体成分へと分解可能な任意の chordal graph に対して，その自己同型群が多項式時間計算可能であることを示した．

(2) 11:30~12:30，2-リンクパズルの多項式時間解法，牧野 格三（東工大）
（概要）ナンバーリンクパズルを「k-リンクパズル」と呼ばれるグラフ論的な計算問題へと一般化し，3 × (偶数) や 4 × (偶数) といった格子グラフに関する 2-リンクパズルに対して多項式時間アルゴリズムを示すとともに，一般の格子グラフに関する予想を述べた．さらに，参加者を交えた討論を経て新たな研究課題が見出された．

(3) 13:30~15:00，On the Laminar Structure of Ptolemaic and Distance Hereditary Graphs，上原 隆平 (JAIST)，宇野裕之 (大阪府立大学)
（概要）Chordal graph（のクラス）と distance hereditary graph（のクラス）の共通部分として特徴付けられている Ptolemaic graph（のクラス）に対して，ある種の木表現モデルが存在すること，その木表現モデルが各 Ptolemaic graph に対して一意的に定まること，ならびに，その木表現モデルを線形時間で構築できることを示した．さらに，この結果をもとに，Ptolemaic graph（のクラス）に対する認識問題や同型性判定問題が線形時

間計算可能であることを示した．また，この研究の発展的可能性として，distance hereditary graph に対する同様の木表現モデルの存在性に関する予想を述べた．

(4) 15:15~16:45，On precoloring extension problem，名古屋孝幸（東京電機大学）
（概要）グラフの precoloring extension problem (PREXT と略す) に対して，一般のグラフに対しては NP 完全であることや，クリーク数を制限した chordal graph に対して多項式時間計算可能であることを紹介した．また，PREXT を制限した 1-PREXT 問題に対して，chordal graph に対するネットワークフローを用いた多項式時間アルゴリズムを紹介した．

研究発表終了後，午後 6 時頃まで討論を行った．討論の間に，グラフ自己同型群問題の応用研究として，河内亮周氏（東工大）に次の成果を発表して頂いた．

(5) Computational Distinguishability between Quantum States and Its Applications，A. Kawachi, T. Koshiba, H. Nishimura and T. Yamakami
（概要）確率分布に対する判別問題の自然な一般化として，二つの量子状態を判別する問題（QSCDff）を新たに定義し，その問題が落とし戸関数の性質を有すること，その最悪計算量と平均計算量が等価であること，さらに，その最悪計算量がグラフ自己同型群問題の最悪計算量と同等以上であることを示した．

各地から多くの参加者を得て活発な討論が行われ，発展的研究課題を見出すこともできて，とても充実した研究集会であった．

研究業績一覧

学術論文

1. T. Onodera and K. Tanaka:
"Shuffle for Paillier's Encryption Scheme", IEICE Transactions on Fundamentals, Special Section on Discrete Mathematics and Its Applications, （掲載予定）.
概要: In this paper, we propose a proof scheme of shuffle, which is an honest verifier zero-knowledge proof of knowledge such as the protocols by Groth and Furukawa. Unlike the previous schemes proposed by Furukawa-Sako, Groth and Furukawa, our scheme can be used as the shuffle of the elements encrypted by Paillier's encryption scheme, which has an additive homomorphic property in the message part. The ElGamal encryption scheme used in the previous schemes does not have this property.

2. J. Cai and O. Watanabe:
"Relativized collapsing between BPP and PH under stringent oracle access.", Information Processing Letters, 90(3), 147-154, May, 2004.
概要: We propose a new model of stringent oracle access defined for a general complexity class. For example, when comparing the power of two machine models relative to some oracle set X, we restrict that machines of both types ask queries from the same segment of the set X. In particular, for investigating polynomial-time (or polynomial-size) computability, we propose polynomial stringency, bounding query length to any fixed polynomial of input length. Under such stringent oracle access, we show an oracle G such that $\mathrm{BPP}^G = \mathrm{PH}^G$.

3. J. Cai and O. Watanabe.:
"On proving circuit lower bounds against the polynomial-time hierarchy", SIAM Journal on Computing, 33(4), 984-1009, 2004.
概要: We consider the problem of proving circuit lower bounds against the polynomial-time hierarchy. We give both positive and negative results. For the positive side, for any fixed integer $k > 0$, we give an explicit SIGptwo language, acceptable by a SIGptwo-machine with running time

$O(n^{k^2+k})$, that requires circuit size $> n^k$. This provides a constructive version of an existence theorem of Kannan. Our main theorem is on the negative side. We give evidence that it is infeasible to give relativizable proofs that any single language in the polynomial-time hierarchy requires super polynomial circuit size. Our proof techniques are based on the decision tree version of the Switching Lemma for constant depth circuits and Nisan-Wigderson pseudorandom generator. We also take this opportunity to publish some unpublshed older results of the first author on constant depth circuits, both straight lower bounds and inapproximability results based on decision tree type Switching Lemmas.

4. R. Uehara, S. Toda, T. Nagoya:
"Graph Isomorphism Completeness for Chordal Bipartite Graphs and Strongly Chordal Graphs", Discrete Applied Mathematics, 145(3), 479–482, January, 2005.
概要: This paper deals with the graph isomorphism (GI) problem for two graph classes: chordal bipartite graphs and strongly chordal graphs. It is known that GI problem is GI complete even for some special graph classes including regular graphs, bipartite graphs, chordal graphs, comparability graphs, split graphs, and k-trees with unbounded k. On the other hand, the relative complexity of the GI problem for the above classes was unknown. We prove that deciding isomorphism of the classes are GI complete.

研究会等

1. R. Hayashi and K. Tanaka:
"The Sampling Twice Technique for the RSA-based Cryptosystems with Anonymity", PKC 2005—The 8th International Workshop on Practice and Theory in Public Key Cryptography, Lecture Notes in Computer Science 3386, 216-233, January, 2005.
概要: We say that an encryption scheme or a signature scheme provides anonymity when it is infeasible to determine which user generated a ciphertext or a signature. To construct the schemes with anonymity, it is necessary that the space of ciphertexts or signatures is common to each user. In this paper, we focus on the techniques which can be used to obtain this anonymity property, and propose a new technique for obtaining the anonymity property on RSA-based cryptosystem, which we call "sampling twice." It generates the uniform distribution over $[0, 2^k)$ by sampling the two elements from $\mathbb{Z}_N$ where $|N| = k$. Then, by applying the sampling twice technique, we construct the schemes for encryption, undeniable and confirmer signature, and ring signature, which have some advantage to the previous schemes.

2. 鈴木学, 田中圭介:
"ランダムオラクルモデルを用いたプロトコルの指標と方式", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 1, 151-156, 2005 年 1 月.
概要: A study of the random oracle model seems to be concentrated to showing the gap between the schemes in the random oracle model and the schemes whose random oracles are replaced with functions chosen at random from some function ensembles. We consider a different direction on the study of the schemes in the random oracle model. We focus on the size of the tables necessary to describe all of the entries to be potentially queried in the random oracle model. We show how to reduce the table sizes of the schemes for encryption and signature in the random oracle model. In particular, we apply this idea to PSS-R and OAEP and show the security of our

schemes.

3. 金内志津, 田中圭介:
   “Computational Bilinear Diffie-Hellman 問題に基づく複数キーワード検索つき公開鍵暗号方式”, 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 1, 343-348, 2005 年 1 月.
   概要: Park, Kim, and Lee proposed a public-key encryption with conjunctive field keyword search (PECK). They proposed two constructions for PECK based on the Decisional Bilinear Diffie-Hellman problem. We construct a variant of one of their schemes based on the Computational Bilinear Diffie-Hellman problem.

4. 樋渡玄良, 田中圭介:
   “Cramer-Shoup の構成法による平方剰余問題と関連する暗号方式”, 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 2, 481-486, 2005 年 1 月.
   概要: At Eurocrypt ’02 Cramer and Shoup proposed a general paradigm to construct practical public-key cryptosystems secure against the adaptive chosen ciphertext attack as well as several concrete examples. Using the construction, we present a new variant of the Cramer-Shoup encryption scheme, secure against the adaptive chosen ciphertext attack. Our variant is based on the problem related to the quadratic residuosity (QR). They also proposed the encryption scheme based on the QR, but this scheme is less efficient than those based on the decision Diffie-Hellman problem or the decision composite residuosity. In this paper, we define the new assumptions related to the QR assumption and propose a new public-key encryption scheme whose security is based on the new assumption. Our scheme is more efficient than the QR-based scheme proposed by Cramer and Shoup.

5. 小野寺貴男, 田中圭介:
   “中程度の難しさをもつ関数のモデルと方式”, 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 2, 799-804, 2005 年 1 月.
   概要: Moderately-hard functions are useful for many applications and there are quite many papers concerning on moderately-hard functions. However, the formal model for moderately-hard functions have not been proposed. In this paper, first, we propose the formal model for moderatelyhard functions. For this purpose, we construct the computational model and investigate the properties desired for moderately-hard functions. Then, we propose that some particular functions can be used as moderately-hard functions. These functions are based on two ideas: the difficulty of factoring $p^r q$ and sequential computation of primitive functions.

6. 羽田大樹, 田中圭介:
   “認証付き鍵交換プロトコルにおける non-malleability に基づく安全性”, 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 3, 1087-1092, 2005 年 1 月.
   概要: This paper continues the study of password-based protocols for authenticated key exchange (AKE). In 2000, Bellare, Pointcheval, and Rogaway proposed the formal model on AKE. In this paper, we propose the new security notions on AKE, based on the non-malleability of session keys. Then we prove that this security notion is equivalent to that proposed by Bellare, Pointcheval, and Rogaway. Furthermore, we show that there is a protocol secure in the random oracle model not always secure in the standard model with collision-resistant hash functions.

7. 林良太郎, 田中圭介:
   “ElGamal 暗号と Cramer-Shoup 暗号をもとにした匿名性を持つ暗号方式”, 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 3, 1315-1320, 2005 年 1 月.
   概要: In this paper, we have proposed

new variants of the ElGamal and the Cramer-Shoup encryption schemes. Our schemes have the anonymity property even if each user chooses an arbitrary prime q where $|q| = k$ and $p = 2q + 1$ is also prime. More precisely, our ElGamal variants provide anonymity against the chosen-plaintext attack, and our Cramer-Shoup variants provide anonymity against the adaptive chosen-ciphertext attack. These anonymity properties are proved under a slightly weaker assumption than the DDH assumption. Furthermore, our ElGamal variants are secure in the sense of IND-CPA, and our Cramer-Shoup variants are secure in the sense of IND-CCA2.

8. 林良太郎, 田中圭介:
"匿名性をもつ RSA 暗号方式のための Sampling Twice テクニック", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 3, 1321-1326, 2005 年 1 月.
概要: We say that an encryption scheme or a signature scheme provides anonymity when it is infeasible to determine which user generated a ciphertext or a signature. To construct the schemes with anonymity, it is necessary that the space of ciphertexts or signatures is common to each user. In this paper, we focus on the techniques which can be used to obtain this anonymity property, and propose a new technique for obtaining the anonymity property on RSA-based cryptosystem, which we call "sampling twice." It generates the uniform distribution over $[0, 2^k)$ by sampling the two elements from $\mathbb{Z}_N$ where $|N| = k$. Then, by applying the sampling twice technique, we construct the schemes for encryption, undeniable and confirmer signature, and ring signature, which have some advantages to the previous schemes.

9. 三原章裕, 田中圭介:
"指定検証者署名への変換が可能な Aggregate Signature", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 3, 1453-1458, 2005 年 1 月.
概要: There is a signature scheme which can aggregate two or more persons ' signatures to one, called an aggregate signature. In this paper, we propose a scheme of an aggregate signature which has additional functionality allowing any holder of a signature to designate the signature to any desired designated-verifier. By this functionality, no one other than the designated-verifier can verify the signature, so the signature passed to other persons would not appear where the signer does not intend to send it in the form which anyone can verify.

10. K. Hatano and O. Watanabe:
"Learning r-of-k functions by boosting", 15th International Conference on Algorithmic Learning Theory (ALT 2004), Lecture Notes in Computer Science 3244, 114-126, 2004.
概要: We investigate further improvement of boosting in the case that the target concept belongs to the class of r-of-k threshold Boolean functions, which answers "+1" if at least r of k relevant variables are positive, and answers "−1" otherwise. Given m examples of a r-of-k function and literals as base hypotheses, popular boosting algorithms (e.g., AdaBoost) construct a consistent final hypothesis in $O(k^2 \log m)$ iterations. While this convergence speed is tight in general, we show that a modification of AdaBoost (confidence-rated AdaBoost or InfoBoost) can make use of the property of r-of-k functions that make less error on one-side to find a consistent final hypothesis in $O(kr \log m)$ iterations. Our result extends the previous investigation by Hatano and Warmuth and gives more general examples where confidence-rated AdaBoost or InfoBoost has an advantage over AdaBoost.

11. O. Watanabe:
“Pseudo expectation: A tool for analyzing local search algorithms”, Statistical Physics of Disordered Systems and its Applications (SPDSA2004), July, 2004.
概要: Watanabe et. al. proposed pseudo expectation for analyzing relatively simple Markov processes, which would be often seen as simple execution models of local search algorithms. In this paper, we first explain how it is used, and then investigate the approximation error bound of pseudo expectations.

12. 新倉 康明, J. Schneider, 渡辺 治.:
“単純な規則で表されるマルコフ過程の近似解析手法”, アルゴリズム研, 情処研報 AL94, 73-80, 2004.
概要: 本稿では，単純で比較的状態数の大きなマルコフ過程のモデルを設定し，その平均的な状態遷移を，簡単な計算 (これを疑似平均と呼ぶことにする) で近似する手法を提案する．乱択アルゴリズムの動きは，マルコフ過程のモデルで近似することができる場合がある．しかし，マルコフ過程としても状態空間が大きくなるために，その平均的な振る舞いの解析が非常に困難になる場合が多い．そのような解析を簡単な計算で行うための道具が疑似平均である．本稿では，幾つかの実験と解析を通して，疑似平均の近似性能について考察する．

学会大会等

1. O. Watanabe:
“Pseudo expectation: A tool for analyzing local search algorithms”, Optimization algorithms and quantum disordered systems, 2004.

B03: 量子論理回路の最適化に関する研究

西野 哲朗　垂井 淳

電気通信大学 電気通信学部 情報通信工学科
〒 182-8585 調布市調布ヶ丘 1-5-1
{nishino,tarui}@ice.uec.ac.jp

1　はじめに

分子レベルのミクロの世界では, 現在の理論に基づく集積回路はそのままでは機能しなくなる. このため, ２０年後には, 現在の半導体技術はその物理的限界に突き当たると言われている. したがって, 将来, 単一分子デバイス等を用いて, コンピュータを極限までミクロ化し, 高速化するためには, まったく新しい理論に基づく計算機アーキテクチャが必要となる. そのような新たなコンピュータとして, 近年, 量子コンピュータが注目されている.

量子コンピュータは, 最終的に量子論理回路として実現されるが, 量子論理回路設計の基礎理論はまだ構築できていない. 量子論理回路の場合, 実現可能な量子ビット数には限りがあり, また, デコヒーレンスという物理現象が生じる前に計算を終了させる必要があるため, 回路の段数も小さくしなければならない. このような, 量子ビット数（ワイヤ数）と回路の段数をうまくバランスさせて削減し, 最適な量子論理回路を自動設計するための基礎理論を構築して行くことが, 本研究の目的である.

一方で, 近年，NMR やイオントラップ，単一光子，量子ドットなどを用いて量子 Turing 機械を物理的に実現し，量子計算機を構築しようという研究が盛んに行なわれている．なかでも，NMR（Nuclear Magnetic Resonance, 核磁気共鳴）を用いた量子計算は，近い将来に実現可能であると考えられている．NMR 法は，分子を構成する原子一つ一つを区別して見ることを可能にする方法で，現在，有機化合物の分子構造解析の分野で威力を発揮している．しかし， このような NMR 装置を用いて行う **NMR 量子計算**は，通常の量子計算とは若干異なり， **Bulk 量子計算**と呼ばれる枠組みであるため，NMR 量子計算の理論的基礎を与えるための研究も行われている [6, 7, 8].

特に，文献 [7] では， NMR 量子計算が通常の量子計算よりも効率的である可能性が（計算モデルを用いずに）定性的に指摘されている．しかし，このような議論は， 明確な計算モデル上で行わなければならない．なぜなら， 例えば， NMR 量子計算機が， 出力値に対する無限の測定精度を持つと仮定すると，論理式の充足可能性判定問題（SAT）が多項式時間で解けるという非現実的な結果が導き出されてしまうからである．実際の NMR 装置には， 測定精度に関する厳しい制約があるため，NMR 量子計算のアルゴリズムの効率について理論的に考察する際には，このような測定精度を十分考慮に入れる必要がある．

そこで，今年度の本研究では，このような NMR 量子計算の枠組みを反映させた Bulk 量子計算モデルを提案し，その性質について考察した．具体的には，出力値の測定精度について厳密な制約を設けても，Bulk 量子計算モデル上では， Grover のアルゴリズムの効率が改善できることを示した. この研究成果を応用すれば, 将来的に, NMR 量子計算を実行するサイズの小さな量子回路の設計も可能になるものと期待される. 以下では, 学術論文 1 で示した, この研究内容を詳しく紹介する.

2　Bulk 量子計算

1985 年に，英国人物理学者 David Deutsch は，**量子回路**（quantum circuit）という量子力学的動作原理に基づく新たな計算モデルを提案した [3]. この量子回路によって構成された計算機が，**量子計算機**と呼ばれている.

通常の組合わせ論理回路の 1 本のワイヤには，

0 または 1 が保持できるが，量子回路の 1 本のワイヤには，0 と 1 の任意の重ね合わせ状態が保持できる．ここで，重ね合わせ状態とは，0 に対応する状態ベクトル $|0\rangle$ と 1 に対応する状態ベクトル $|1\rangle$ を，それぞれ，

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

とするとき，$\alpha|0\rangle + \beta|1\rangle$ の形で表されるベクトルの和のことをいう．ただし，α と β は，条件式 $|\alpha|^2 + |\beta|^2 = 1$ を満たす任意の複素数であり，振幅と呼ばれる．この重ね合わせ状態を**観測**すると，0（または 1）が確率 $|\alpha|^2$（$|\beta|^2$）で読めるものと仮定する．

量子回路の 1 本のワイヤが保持できる情報量を**1 量子ビット**（quantum bit, qubit）という．量子回路の動作は，量子ビットに対するユニタリ変換と呼ばれる線形変換の適用という形で表現できる．一方，量子回路上で実行されるアルゴリズムを**量子アルゴリズム**と呼ぶ．そこで以下では，量子アルゴリズムを量子ビットに適用されるユニタリ変換の系列として記述することにする．

本論文では，近い将来に比較的容易に実現可能と思われている，NMR 量子計算をモデル化した**Bulk 量子計算**について考察する．Bulk 量子計算と通常の量子計算の相違は，計算結果の**観測**の規約が以下のように異なっている点にある．一般に量子回路の出力は，量子ワイヤ上に，$\alpha|0\rangle + \beta|1\rangle$ という形の重ね合わせ状態として保持される．

通常の量子計算の場合，この重ね合わせ状態 $\alpha|0\rangle + \beta|1\rangle$ を観測すると，0（または 1）が確率 $|\alpha|^2$（$|\beta|^2$）で読めるものと仮定される．一方，NMR 量子計算などの Bulk 量子計算においては，同じ重ね合わせ状態を測定すると，$|\beta|^2 - |\alpha|^2$ という実数値が測定できるものと仮定される．ただし，その際には測定誤差 $\varepsilon > 0$ が存在し，重ね合わせ状態 $\alpha\,|0\rangle + \beta\,|1\rangle$ にある量子ビットを測定すると，実際には，以下の関係式

$$|\beta|^2 - |\alpha|^2 - \varepsilon \leq \theta \leq |\beta|^2 - |\alpha|^2 + \varepsilon \qquad (2.8)$$

を満す実数値 θ が読み出せるという精度保証がなされているものと仮定する．

ただし，この ε は回路の入力数に依存する値であり，さらに，NMR 量子計算におけるサンプル数のような，計算装置ごとに定まるパラメータにも依存する値として，各量子回路ごとに指定される値であるとする．

本論で提案する Bulk 量子計算モデルは，通常の量子回路において，その出力値の読み出しに，上記の規約を仮定する．

また，Bulk 量子計算における測定では，波束が収縮しないので，重ね合わせ状態を乱さずに測定を行なうことができると仮定する．

ここで ε は 1 以下の定数であるが，例えば NMR 装置の測定精度の場合，$4 \sim 5$ 量子ビットの Grover のアルゴリズムの実験においては，ε の値が $\frac{1}{8}$ 以下と仮定できると言われている．ただし，この ε の値は，現在の液体 NMR を用いた実験におけるものであり，固体 NMR その他を用いた将来の Bulk 量子計算装置においては，ε の値がさらに改善されていくものと期待されている．

3 Grover のアルゴリズム

いま，$0 \leq r \leq 2^n - 1$ なる整数 r の集合を定義域とする関数 f を考える．すなわち，f の定義域には 2^n 個の整数が含まれている．この定義域のなかに，特別な整数 r_0 が存在して，$x = r_0$ のときのみ $f(x) = 1$ となり，それ以外の x に対しては $f(x) = 0$ となるものとする．関数 f に対する**オラクル**とは，f の定義域に属する整数 x が入力として与えられると，$f(x)$ の値（0 または 1）を返すブラックボックスのことをいう．また，関数 f に対する**量子オラクル**とは，f の定義域に属する整数 x の重ね合わせ $\alpha_1\,|x_1, 0\rangle + \alpha_2\,|x_2, 0\rangle + \cdots + \alpha_N\,|x_N, 0\rangle$ が入力として与えられると，$f(x)$ の値（0 または 1）の重ね合わせ $\alpha_1\,|x_1, f(x_1)\rangle + \alpha_2\,|x_2, f(x_2)\rangle + \cdots + \alpha_N\,|x_N, f(x_N)\rangle$ を返すブラックボックスのことをいう．ここで，任意の入力に対し，量子オラクルは単位時間で出力を返すものと仮定する．

Grover のアルゴリズムが扱う**探索問題**は，以下の通りである．

> **入力：** 量子オラクルとして実現されるブール関数 f の変数の個数 n.
> **問題：** n 変数ブール関数 f に対する量子オラクルが与えられたときに，上記の

条件を満たす r_0 を発見せよ．

この問題を解くために，f の定義域を古典的に探索した場合，r_0 を発見するまでの $f(x)$ の評価回数（オラクル呼び出しの回数）の期待値は 2^{n-1} となる．これに対し，Grover のアルゴリズムでは，このオラクル呼び出しの回数の期待値を，$O\left(\sqrt{2^n}\right) = O\left(2^{n/2}\right)$ にすることができる．本論では， 量子アルゴリズムの実行に必要な時間量を， このようなオラクル呼び出しの回数によって評価するものとする．

論文 [5] で， Grover は， 以下の量子探索アルゴリズムを示した．

1. n 個の量子ビットを，$|00...0\rangle$ から $|11...1\rangle$ のすべての n ビット状態 (S で表す) が等しい振幅を持つ重ね合わせ状態に初期化する．
2. 以下の Grover 変換 G を $O(\sqrt{N})$ 回繰り返す．
   (a) 量子オラクルを呼び出すことにより，上記重ね合わせ状態中の各状態 S に対し，以下の変換を並列実行する．
   - $f(S) = 1$ の場合は**位相反転** を適用する．
   - $f(S) = 0$ の場合は何も行わない．

   (b) 以下のような行列 D により定義される**拡散変換** D を適用する．ただし， $N = 2^n$ とする．

$$D_{ij} = \frac{2}{N} \text{ if } i \neq j \text{ and } D_{ii} = -1 + \frac{2}{N}$$

3. 最終的に得られた状態を測定する．少なくとも，0.5 以上の確率で状態 r_0 が得られる．

上のステップ 2 の部分が Grover のアルゴリズムの核心であり，これによって，所望の状態の振幅を $O\left(\frac{1}{\sqrt{N}}\right)$ ずつ増幅することができる．したがって，ステップ 2 を $O\left(\sqrt{N}\right)$ 回繰り返すことにより，r_0 に対応する所望の状態を得る確率を，1 に近づけることができる．

拡散変換 D は平均についての反転演算として解釈できる．すなわち，上のアルゴリズムで行なっていることは，

a) 所望の状態の振幅の符号を反転させることによって平均値から遠ざけ，

b) 平均値を中心として折り返すことにより，所望の状態の振幅をより大きく，その他の状態の振幅をより小さくすることとして説明できる．

4 Bulk 量子計算モデル上で SAT を解く量子アルゴリズム

本節では，Bulk 量子計算機上で充足性判定問題を解く量子アルゴリズムを示し，その計算量を考察する．

4.1 充足可能性判定問題

本節で取り扱う充足性判定問題（satisfiability problem, SAT）とは，以下のような問題である．

入力：n 変数ブール式 $f(x_1, x_2, \cdots, x_n)$.
問題：$f(x_1, x_2, \cdots, x_n) = 1$ を満足する $(a_1, a_2, \cdots, a_n) \in \{0,1\}^n$ が存在するか否かを判定せよ．

ここで，$\{0,1\}^n$ の中に $f(x) = 1$ を満たす充足解 $x \in \{0,1\}^n$ は全部で t 個含まれているものとする．この t の値は未知であり， $t \ll N$ と仮定する．また，任意の解 x に対し $f(x)$ の計算は単位時間で可能であるものとする．

4.2 アルゴリズムのアイデア

Bulk 量子計算を行う量子回路の先頭の n 量子ビットを等振幅の重ね合わせ状態に設定し，$n+1$ 番目の量子ビットに $f(x)$ の計算結果を書き込んでから，$n+1$ 番目の量子ビットを観測することを考える．このとき，充足解が存在しないならば，重ね合わせ内の $n+1$ 番目の量子ビットに書き込まれている値はすべて 0 であるため，$|\beta|^2 - |\alpha|^2$ の値は -1 となる．一方，充足解が存在するならば， $|\beta|^2 - |\alpha|^2$ の値は -1 より大きな値となる．しかしながら，Bulk 量子計算においては ε の測

定誤差が存在するため，充足解が存在する場合と存在しない場合を区別することができない場合がある．

そこで，Grover 変換を行うことにより，充足割り当てに対応する状態の振幅を増幅した後に，$n+1$ 番目の量子ビットに $f(x)$ の計算結果を書き込み，$n+1$ 番目の量子ビットを測定することを考える．この場合，充足解に対応する状態の振幅が増幅しているため，充足解が存在する場合は，$|\beta|^2 - |\alpha|^2$ の値が，Grover 変換を行わない場合よりも大きな値となる．一方，充足解が存在しない場合は，Grover 変換を行わない場合と同様に $|\beta|^2 - |\alpha|^2$ の値は -1 となる．

このようにして Grover 変換を繰り返し，充足解に対応する状態の振幅を増幅することにより，充足解が存在する場合と存在しない場合を区別することができるようになる．

4.3 アルゴリズム

SAT を解く Bulk 量子計算アルゴリズム BULKSAT の詳細は，以下の通りである．

BULKSAT

[入力]：量子オラクルとして与えられるブール関数 f の変数の個数 n.

[出力]：もし $f(x) = 1$ を満たすような $x \in \{0,1\}^n$ が存在するならば 1 を返す．それ以外の場合は 0 を返す.

[アルゴリズム] アルゴリズム BULKSAT は以下の 5 ステップからなる．

[ステップ 1] $j = 1$ に設定する．ここで，j は Grover 変換の繰り返し回数のカウンタである．$n+1$ 個の量子ビットを，以下のような初期状態に設定する．ただし，$N = 2^n$ とする．

$$\sum_{x=0}^{N-1} \frac{1}{\sqrt{N}} |x\rangle |0\rangle$$

[ステップ 2] 上記の重ね合わせ状態に Grover 変換 G を 1 回適用する (詳細は第 3 節参照)．適用後の状態は以下のようになる．

$$\sum_{x \in N_{ans}} \sqrt{a_j} |x\rangle |0\rangle + \sum_{x \notin N_{ans}} \sqrt{\frac{1-ta_j}{N-t}} |x\rangle |0\rangle$$

ここで N_{ans} は t 個の充足解からなる集合であり，$\sqrt{a_j}$ は Grover 変換を j 回適用した時点での，解である状態の振幅である．

[ステップ 3] $n+1$ 番目の量子ビットに $f(x)$ の値を書き込みむ．すると，以下の重ね合わせ状態が得られる．

$$\sum_{x \in N_{\rm ans}} \sqrt{a_j} |x\rangle |1\rangle + \sum_{x \notin N_{\rm ans}} \sqrt{\frac{1-ta_j}{N-t}} |x\rangle |0\rangle$$

その後，$n+1$ 番目の量子ビットを測定する．得られた測定値を θ_a とする．

[ステップ 4] もし $\theta_a > -1+\varepsilon$ ならば，1 を出力して停止する．そうでないならば，次のステップに進む.

[ステップ 5] もし $j > \sqrt{\varepsilon N}$ ならば，答えとして 0 を出力して停止する．成立していなければ，$j := j+1$ とし，$n+1$ 番目の量子ビットを 0 に戻した後，ステップ 2 へ戻る．

4.4 アルゴリズムの正当性と計算量

上記のステップ 3 で $n+1$ 番目の量子ビットを測定したときの測定値について考える．

まず，充足解が存在するとき，つまり $t \geq 1$ の場合について考える．j 回の振幅増幅を行った結果，充足解に対応する状態の振幅が $\sqrt{a_j}$ となったとする．この場合， 充足解ではない状態の振幅は $\sqrt{\dfrac{1-a_jt}{N-t}}$ となる．

このとき，$|\alpha|^2 - |\beta|^2$ の値は，

$$\left|\sqrt{a_j}\right|^2 t - \left|\sqrt{\frac{1-a_jt}{N-t}}\right|^2 (N-t) = -1 + 2a_jt$$

となる．この値が $-1+2\varepsilon$ を越えていれば，充足解が存在すると判断することができるので，充足解に対応する状態の振幅が $\sqrt{a_j} > \sqrt{\frac{\varepsilon}{t}}$ を満たすようになるまで，Grover 変換を繰り返せばよい．

Grover のアルゴリズムでは，量子オラクルを j 回呼び出した時点での充足解に対応する状態の振幅 $\sqrt{a_j}$ は $\sqrt{a_j} = \frac{\sin((2j+1)\theta)}{\sqrt{t}}$ と表すことができる．ここで，$\sin\theta = \sqrt{\frac{t}{N}}$ である．したがって，

$$\sqrt{a_j} \quad > \quad \sqrt{\frac{\varepsilon}{t}}$$

つまり，

$$\sin((2j+1)\theta) \quad > \quad \sqrt{\varepsilon} \qquad (2.9)$$

を満たす j を求めればよい．また，$\varepsilon \leq \frac{1}{8}$ と仮定すると，$\sqrt{\varepsilon}$ は非常に小さい値とみなすことができる．式 (2.9) を満たす最も小さい j を求めたいので，$\sin((2j+1)\theta)$ も非常に小さい値と考えることができる．よって，$\sin((2j+1)\theta) \simeq (2j+1)\theta$ と近似することができる．また，$\frac{t}{N} \ll 1$ であるので，$\theta = \sqrt{\frac{t}{N}}$ と近似できる．以上のことより，式 (2.9) は，

$$(2j+1)\sqrt{\frac{t}{N}} \quad > \quad \sqrt{\varepsilon}$$

となり，この不等式を解くことにより

$$j \quad > \quad \frac{1}{2}\sqrt{\frac{\varepsilon N}{t}} - \frac{1}{2}$$

を得る．

したがって，$\frac{1}{2}\sqrt{\frac{\varepsilon N}{t}}$ 回 Grover 変換を繰り返せば充足解が存在することを確認できる．

充足解が 1 つでも存在するならば，$\frac{1}{2}\sqrt{\varepsilon N}$ 回 Grover 変換を繰り返すまでに，アルゴリズムは 1 を出力して停止する．したがって，$\frac{1}{2}\sqrt{\varepsilon N}$ 回 Grover 変換を繰り返すまでにアルゴリズムが停止しないならば，充足解は存在しないと判断できる．

このようにして，提案アルゴリズムは $\frac{1}{2}\sqrt{\frac{\varepsilon N}{t}}$ 回の Grover 変換を行うことで，充足可能性判定問題を解く．Grover 変換の 1 回の実行につき，関数 f の値を 3 回評価するため，全体では関数 f を $\frac{3}{2}\sqrt{\frac{\varepsilon N}{t}}$ 回評価すれば良い．

5 BULK 量子計算モデル上の量子探索アルゴリズム（唯一解の場合）

本節では，BULK 量子計算機上における Grover のアルゴリズムの実行について考える．ただし，本節では，所望の解はちょうど 1 つしか存在しないと仮定する．

5.1 アルゴリズムのアイデア

初期状態では $N/2$ 個の 0 と $N/2$ 個の 1 が重ね合わされているため，$|\beta|^2 - |\alpha|^2$ の値は 0 となる．

ここで，Grover 変換を行うことにより，充足解に対応する状態の振幅を増幅した後に，k 番目の量子ビットを測定したとする．この場合，充足解に対応する状態の振幅が増幅されているため，充足解の k ビット目が 1 であるときは，$|\beta|^2 - |\alpha|^2$ の値は，初期状態の値よりも大きな値となる．一方，充足解の k ビット目が 0 であるときは，初期状態の値よりも小さな値となる．Grover 変換を繰り返し，充足解に対応する状態の振幅を増幅することにより，充足解が存在する場合と存在しない場合を区別することができるようになる．

5.2 アルゴリズム

提案アルゴリズム BULKSEARCH1 の詳細は，以下の通りである．

BULKSEARCH1(n)

[入力]：量子オラクルとして与えられるブール関数 f の変数の個数 n.

[出力]：$f(x) = 1$ を満たすような $x \in \{0,1\}^n$.

[アルゴリズム] アルゴリズムは以下の 3 ステ

ップからなる．

[ステップ 1] n 個の量子ビットを以下のような初期状態に設定する．ただし，$N = 2^n$ とする．

$$\sum_{x=0}^{N-1} \frac{1}{\sqrt{N}} |x\rangle$$

[ステップ 2] Grover 変換 G を $\frac{1}{2}\sqrt{\varepsilon N}$ 回適用する．適用後の状態は以下のようになる．

$$\sqrt{a}\,|x_{ans}\rangle + \sum_{x \notin N - x_{ans}} \sqrt{\frac{1-a_j}{N-1}}\,|x\rangle$$

ここで，x_{ans} は充足解，$\sqrt{a}$ は充足解の振幅であるとする．

[ステップ 3] 1 〜 n 番目までの，各量子ビットを測定し，解を決定する．第 k 量子ビットの測定値を θ_k とする．もし $\theta_k > 0$ ならば，解の k ビット目の値を 1 とする．もし $\theta_k < 0$ ならば，解の k ビット目の値を 0 とする．

5.3 アルゴリズムの正当性と計算量

j 回の Grover 変換によって振幅増幅を行い，充足解に対応する状態の振幅が $\sqrt{a_j}$ になったときに，k 番目の量子ビットを測定したとする．充足解の k ビット目の値が 1 であったとすると，k 番目の量子ビットの重ね合わせ状態は，振幅 $\sqrt{a_j}$ を持つ $|1\rangle$ が 1 個と，振幅 $\sqrt{\frac{1-a_j}{N-1}}$ を持つ $|1\rangle$ が $N/2-1$ 個，および，振幅 $\sqrt{\frac{1-a_j}{N}}$ を持つ $|0\rangle$ が $N/2$ 個より構成されている．

このとき，$|\beta|^2 - |\alpha|^2$ の値は，$a_j + \frac{1-a_j}{N-1} * (N/2-1) - \frac{1-a}{N-1} * (N/2) = \frac{a_j N - 1}{N-1}$ となる．この値が閾値 ε を越えていれば，測定値として 0 よりも大きい値を読み出すことができ，解を決定することができる．したがって，$a_j \geq \frac{\varepsilon N - \varepsilon + 1}{N}$ を満たすまで Grover 変換を繰り返せばよい．

また，$\sqrt{a_j} = \sin((2j+1)\theta)$ と表すことができる．ここで，$\sin\theta = \sqrt{\frac{1}{N}}$ である．したがって，

$$\sqrt{a_j} \;>\; \sqrt{\frac{\varepsilon N - \varepsilon + 1}{N}}$$

つまり，

$$\sin((2j+1)\theta) \;>\; \sqrt{\frac{\varepsilon N - \varepsilon + 1}{N}}$$

を満たす j を求めればよい．ε は非常に小さい値であるので，$\sqrt{\frac{\varepsilon N - \varepsilon + 1}{N}}$ も非常に小さい値である．よって，4.4 節と同様に，$\sin((2j+1)\theta) \simeq (2j+1)\theta$ と近似することができる．また，$\frac{1}{N} \ll 1$ であるので，$\theta = \sqrt{\frac{1}{N}}$ と近似できる．以上のことより，4.4 節と同様の変換を行い，

$$j \;>\; \frac{1}{2}\sqrt{\varepsilon N - \varepsilon + 1} - \frac{1}{2}$$

を得る．したがって，$\frac{1}{2}\sqrt{\varepsilon N}$ 回 Grover 変換を繰り返せば，充足解の k ビット目が 1 であることを確定できる．

充足解の k ビット目が 0 である場合の解析も，同様である．

以上により，BULK 量子計算によって Grover のアルゴリズムを実行した場合，$\frac{1}{2}\sqrt{\varepsilon N}$ 回の Grover 変換の適用で十分であることがわかった．したがって，この場合には，通常の量子計算機上で Grover のアルゴリズムを動作させた場合と比べ，より少ない Grover 変換の回数で解を求めることができる可能性がある．

6 BULK 量子計算モデル上の量子探索アルゴリズム（複数解の場合）

第 5 節では解がちょうど 1 つ存在する場合の探索アルゴリズムを提案した．しかし，そのアルゴリズムでは，充足解が複数個存在する場合には，最後に特定の量子ビットを測定しても，0 である充足解と 1 である充足解の確率振幅が打ち消しあい，正しい解を求めることができない．そこで，

本節では，4.3 節のアルゴリズムを利用して，解が 2 個以上存在する場合の解探索を行うことを考える．

6.1 アルゴリズムのアイデア

k 番目の量子ビットの値を 1 に設定した状態で，アルゴリズム BULKSAT を動作させると，k ビット目の値が 1 である充足解が存在するか否かを判定することができる．このとき，もし充足解が存在したならば，それ以後 k ビット目の値を 1 に固定する．逆に，充足解が存在しなかったならば，それ以後 k ビット目の値を 0 に固定する．

上の操作を $k = 1$ から $k = n$ まで繰り返すことにより，最終的にひとつの充足解を発見することができる．

6.2 アルゴリズムの詳細

提案アルゴリズム BULKSEARCH2 は以下の通りである．ただし，そのアルゴリズム中で用いる BULKSAT2 については，後から説明する．

BULKSEARCH2(n)

[入力]：量子オラクルとして与えられるブール関数 f の変数の個数 n.

[出力]：$f(x) = 1$ を満たす充足解 $x \in \{0,1\}^n$. ただし，充足解は全部で t 個存在するものとし，$t \geq 2$ の値は未知であるとする．

[アルゴリズム] 1 から n までの i に対し，以下のステップ 1 から ステップ 3 までを繰り返す．

[ステップ 1] $x_i = 1$ に設定し，次のような均等な重ね合わせ状態を生成する．

$$|X_i\rangle = \sum_{x_n=0}^{1} \cdots \sum_{x_{i+1}=0}^{1} \frac{1}{\sqrt{2^{n-i}}} |x_n \cdots x_{i+1} 1 y_{i-1} \cdots y_1\rangle |0\rangle .$$

ここで $y_{i-1}, \cdots, y_1$ はすでに固定された値とする．

[ステップ 2] 以下で述べるサブルーチン BULKSAT2($n - i, 1y_{i-1} \cdots y_1$) を呼び出す．ここで，BULKSAT2($n - i, 1y_{i-1} \cdots y_1$) は $f(y_n \cdots y_{i+1} 1 y_{i-1} \cdots y_1) = 1$ となる $y_n \cdots y_{i+1} \in \{0,1\}^{n-i}$ が存在するとき，かつ，そのときに限り 1 を返し，さもなければ，0 を返す．

[ステップ 3] BULKSAT2($n - i, 1y_{i-1} \cdots y_1$) の出力値を y_i の値に設定し，$i := i + 1$ とする．

[ステップ 4] 充足解 $y_n \cdots y_1$ を出力して停止する．

ここで，アルゴリズム BULKSAT2 の詳細は，以下の通りである．

BULKSAT2(q, z)

[入力]：q および $z \in \{0,1\}^{n-q}$.

[出力]：もし $f(m' \circ z) = 1$ を満たすような $m' \in \{0,1\}^q$ が存在するならば，1 を返す（$\circ$ は記号列の連結を表す）．さもなければ，0 を返す．ここで，下位ビットが z である f の充足解は全部で t' 個あるものとし，t' の値は未知であるとする．

[アルゴリズム] アルゴリズム BULKSAT2 は以下の 5 ステップからなる．

[ステップ 1] $j = 1$ に設定する．ここで，j は Grover 変換の繰り返し回数のカウンタである．以下のような初期状態を生成する．

$$\sum_{m=0}^{2^q-1} \frac{1}{\sqrt{2^q}} |m\rangle |0\rangle$$

[ステップ 2] Grover 変換 G を適用する．適用後の状態は以下のようになる．

$$\sum_{m \in M_{\rm ans}} \sqrt{a_j} |m\rangle |0\rangle + \sum_{m \notin M_{\rm ans}} \sqrt{\frac{1 - t a_j}{2^q - t}} |m\rangle |0\rangle$$

ここで M_{ans} は t' 個の充足解からなる集合であり，$\sqrt{a_j}$ は充足解に対応する状態の振幅である．

[ステップ 3] $(k+1)$ 番目の量子ビットに $f(m \circ z)$ の値を書き込み，$(k+1)$ 番目の量子ビットを観測する．測定値が θ_a であったとする．

$$\sum_{m \in M_{\mathrm{ans}}} \sqrt{a_j} \left|m\right\rangle \left|1\right\rangle + \sum_{m \notin M_{\mathrm{ans}}} \sqrt{\frac{1-ta_j}{2^q - t}} \left|m\right\rangle \left|0\right\rangle$$

[ステップ 4] もし $\theta_a > -1+\varepsilon$ ならば，1 を出力する．さもなければ，次のステップに進む．

[ステップ 5] $j > \sqrt{\varepsilon 2^q}$ であれば，0 を出力する．さもなければ，$j := j+1$ とし，$(k+1)$ 番目の量子ビットを 0 に戻した後，ステップ 2 へ戻る．

6.3 アルゴリズムの計算量

i ビット目の値を決定する際の，BULKSAT2 の実行時における探索空間のサイズは $N/2^i$ であるため，高々 $\frac{1}{2}\sqrt{\frac{\varepsilon N}{2^i}}$ 回，Grover 変換を繰り返すことにより，充足解が存在するか否かを判定することができる．このようにして，1 ビット目から n ビット目までの値を決定するためには，全体として $\sum_{k=1}^{n} \frac{1}{2}\sqrt{\frac{\varepsilon N}{2^k}} < \frac{\sqrt{2}-1}{2}\sqrt{\varepsilon N}$ 回の Grover 変換を行えばよい．1 回の Grover 変換につき，関数 f を 3 回評価しなければならないため，アルゴリズム全体としては，最悪 $\frac{3(\sqrt{2}-1)}{2}\sqrt{\varepsilon N}$ 回 f の評価を行う必要がある．

7 まとめ

本稿では， Bulk 量子計算モデル上における Grover のアルゴリズムの繰り返し回数（オラクル呼び出しの回数）について， さまざまな角度から考察を行ってきた．第 2 節において，Bulk 量子計算においては，実数値 θ は式 (2.8) を満たす値として読み出すことができるとした．そこで，以下では，この θ が式 (2.8) の満たす値として確実に読み出すことができる場合と，確実には読み出すことができないが，高い確率では読み出すことができる場合とに分けて評価を行う．ここで，θ の値が確実に読み出せるか否かは，Bulk 量子計算モデルの実装に依存して決る．

θ の値をある精度内の値として，確実に読み出すことができる場合，Bulk 量子計算モデル上で，本論で示したアルゴリズム BULKSEARCH2 を動作させれば，誤り確率 0 で正解を得ることができる．しかも， そのときに必要な繰り返し回数は $O\left(\sqrt{N}\right)$ 回である．通常の量子計算機では確率 1 で解を発見するには $O(N)$ 回の繰り返しが必要であるため，Bulk 量子計算モデルは，通常の量子計算モデルよりも効率的に計算を行えることがわかる．

一方，θ の値をある精度内の値として確実には読み出すことができないが，高い確率で読み出すことができる場合を考える．この場合，提案アルゴリズムには誤り確率が存在する．解が複数個あるとき，通常の量子計算機と比べ， BULKSEARCH2 は $O(\sqrt{t})$ 倍の繰り返しが必要となってしまう．しかし，その場合でも，解の個数が 1 つのときには，BULKSEARCH1 は通常の量子計算モデルよりも定数倍効率的に計算を行える．

参考文献

[1] Bernstein, E. and Vazirani, U.: Quantum Complexity Theory, *Proc. 25th ACM Symposium on Theory of Computing*, pp. 11–20 (1993).

[2] Deutsch, D.: Quantum Theory,the Church-Turing Principle and the Universal Quantum Computer, *Proc. R. Soc. Lond.*, Vol. A 400, pp. 97–117 (1985).

[3] Deutsch, D.: Quantum Computational Networks, *Proc. R. Soc. Lond.*, Vol. A 400, pp. 97–117 (1985).

[4] Shor, P.W.: Algorithms for Quantum Computation : Discrete Log and Factoring, *in*

Proceedings of the 35th Anniual IEEE Symposium on Foundations of Computer Science (1994).

[5] Grover, L.K.: Quantum Mechanics Helps in Searching for a Needle in a Haystack, *Physical Review Letters*, Vol. 79, No. 2, pp. 325–328 (1997).

[6] Nishino, T.: Mathematical Models of Quantum Computation, *New Generation Computing*, Vol. 20, pp. 1–9 (2002).

[7] Collins, D.: Shortening Grover's search algorithm for an expectation value quantum computer, *quant-ph/0209148* (2002).

[8] Ohta, K., Nishino, T., Okubo, S. and Kunihiro, N.: A Quantum Algorithm using NMR Computers to Break Secret-Key Cryptosystems, *New Generation Computing*, pp. 347–361 (2003).

[9] Beals, R., Buhrman, H., Cleve, R., Mosca, M. and de Wolf, R.: Quantum Lower Bounds by Polynomials, *quant-ph/9802049* (1998).

研究業績一覧

学術論文

1. 大久保誠也, 西野哲朗, 太田和夫, 國廣昇: "Bulk 量子計算モデル上における Grover のアルゴリズムの繰り返し回数について", 情報処理学会論文誌:数理モデル化と応用, (掲載予定).
   概要: 本論文では，NMR 量子計算機をモデル化した，Bulk 量子計算モデル上で動作する，Grover のアルゴリズムの繰り返し回数について考察する．最初に，Bulk 量子計算モデル上で Grover のアルゴリズムを用いて論理式の充足可能性判定問題 (SAT) を解くのに必要となる繰り返し回数について議論する．次に，解がただ一つのみ存在する探索問題に対する量子アルゴリズムを提案する．また，この探索アルゴリズムの秘密鍵探索問題に対する応用についても述べる．さらに，解が複数存在する探索問題に対する量子アルゴリズムも提案する．以上の考察から，本論で提案する Bulk 量子計算モデルは，通常の量子計算モデルよりも Grover のアルゴリズムを高速に実行できる場合があることがわかる．

2. T. Itoh, Y. Takei, and J. Tarui: "Constructing Families of epsilon-Approximate k-Wise Independent Permutations", IEICE Transactions on Fundamentals, vol. E87-Ak, no. 5, pp.993–1103, 2004.
   概要: 一様ランダムな独立ビット列の使用がアルゴリズム設計において有用であることはよく知られており, また, 計算論的暗号理論においてはランダムビットは本質的に必要となるシナリオが多い. 暗号においては量子力学的不確実性を利用する量子暗号も活発に研究されている. このような視点にたつとランダムビット列は計算資源のひとつと考えられる. そしてこの計算資源に関して, 節約する手法の開発と節約できる限界を明らかにすることが重要となる. 以上の視点での研究においては主に次のような設定で議論する. 一様ランダムな独立ビット列を「真のランダム (truly random)」と呼ぶとしこの真のランダムビット列が満たすいくつかの有用な条件を特定する. そしてこの条件は満たしているビット列の集合の構築法とその限界を考える. このようなものは「擬似ランダム (pseudorandom)」と呼ばれる. 関数に関しては, ある種の擬似ランダム性をもつ関数族の容易な構成法が知られている. しかし置換に対しては似たような構成法として知られていることは極めて限られている. 擬似ランダム置換の応用としては暗号が特に重要なものである. 置換に関して我々が扱った問題は次のようなものである. n 個の要素の置換の集合, すなわち, 置換族で, ある種の擬似ランダム性をもつものの構成法およびその限界を明らかにする. 特に, 任意の k 個の要素について, 置換族からランダムに選んだ置換によってその k 個がある k 対に移される確率が, 真にランダムな置換族 ($n!$ のサイズのすべての置換の集合）を用いた場

合と比較して, 差が ε 以下であることを要求する場合を考える. 本論文においては, 擬似ランダム置換族のサイズをどこまで小さくできるかの限界・下界について, ε と k に依存するものを示した.

研究会等

1. Seiya Okubo, Tetsuro, Nishino, Kazuo Ohta, Noboru Kunihiro:
   "A Quantum Algorithm for finding the Minimum on NMR Quantum Computers", ERATO Workshop on Quantum Information Science 2004, pp.152–153, September 1-5, 2004.
   概要: In this paper, we discuss the computational complexity of the minimum finding problem on NMR (Nuclear Magnetic Resonance) quantum computers (NMRQCs for short) with the measurement accuracy ε. Namely, we propose a new quantum algorithm for finding the minimum on NMRQCs. Since, the proposed algorithm can find the minimum with probability 1 using $O(\sqrt{N}\log N)$ oracle queries, we can conclude that NMRQCs are more efficient than ordinary quantum computers in some situation.

2. Hisashi Matsumoto, Seiya Okubo, Tetsuro Nishino:
   "The Computational Capabilities of Quantum Neural Networks", International Workshop on Modern Science and Technology, 2004 September, Kitami, Japan, pp.226-229, September, 2004.
   概要: In 1985, David Deutsch introduced quantum Turing machines (QTMs for short) as Turing machines which can perform so called quantum parallel computations. Then, in 1994, Peter Shor showed that QTM can factor integers with arbitrary small error probability in polynomial time. Since it is widely believed that any deterministic Turing machines cannot factor integers in polynomial time, it is very likely that QTM is an essentially new model of computation. On the other hand, many researchers are studying how to physically implement quantum computers based on QTM. Among others, NMR (Nuclear Magnetic Resonance) offers an appealing prospect for implementation of quantum computers because of a number of reasons. But, quantum computations performed on NMR is slightly different from those performed on QTMs. So, in this paper, we first develop a theory of bulk quantum computation including NMR quantum computation. For this purpose, we define bulk quantum Turing machine (BQTM for short) as a model of bulk quantum computation. Recently, in the field of theory of quantum computation, various kinds of quantum neural networks are proposed. But, it seemed that most of them are not reasonable models of quantum computations. In this paper, we also propose a quantum threshold gate as a basic component of our quantum neural network model. Then, we show that the circuits which consist of these quantum threshold gates can be simulated by ordinaly QTMs. Therefore, we can conclude that our quantum neural network model is a reasonable model of quantum computation. Next, we show that the EXOR function can be learned by a one layer quantum perceptron by using BQTM. It is well known that the EXOR function cannot be learned by a one layer ordinary perceptron. Furthermore, we show some other results on the general computational capabilities of our quantum neural networks.

3. Seiya Okubo, Tetsuro Nishino, Noboru Kunihiro, Kazuo Ohta:
   "On the Inversion Problem of One-way Functions using NMR Quantum Computers", 2004年 暗号と情報セキュリティシンポ

ジウム（SCIS2004）, Jan. 27-30, 2004..
概要: In this paper, we propose two efficient quantum algorithms suitable for NMR quantum computers in order to solve the search problem. In our previous work, a quantum algorithm for the inversion problem of one-way permutations which has only one solution is shown. In this paper, we extend this algorithm to the search problem with multiple solutions. We assume that we use only NMR computers. For this purpose, we first introduce a theory of bulk quantum computation including NMR quantum computation. The first algorithm employs Grover operation in order to obtain the solution with probability 1. Though the second algorithm is slower than the first algorithm, we can run this algorithm in classical parallel manner. We also pointed out its application to codebreak of secret-key cryptosystems.

4. T. Itoh, T. Nagatani, and J. Tarui:
“Explicit Construction of k-Wise Nearly Random Permutaions by Iterated Feistel Transform”, 電子情報通信学会コンピュテーション研究会, 2004-7(2004-4), pp.45–52, 2004.
概要: 上記, 学術論文 2 においては, 擬似ランダム置換族のサイズをどこまで小さくできるかの限界・下界について, ε と k に依存するものを示したが, 本研究報告においては, 任意の k についてこれをコンスタントと考える場合, $(1/\varepsilon)$ と n に関する多項式で押さえられるサイズの置換族を構成する新しい方法を明らかにした.

5. A. Miyata, J. Tarui, and E. Tomita:
“ Learning Boolean Functions in AC_0 on Attribute and Classification Noise”, The 15th Algorithmic Learning Theory, Lecture Notes in Computer Science, vol. 3244, pp.142–155, 2004.
概要: 深さ定数, unbounded fan-in の AND/OR ゲートと否定によって計算可能なブール関数の族は AC_0 と呼ばれる. この族に属する関数に関する学習アルゴリズムは活発に研究されてきた. 特に入力に対する確率分布が一様である場合については学習が可能であるというポジティブな結果がいくつかのシナリオで示されてきた. この論文においては, ある種のノイズが観察データに加わるモデルにおけるアルゴリズムの構成法を明らかにした. 特に, ノイズ率が学習アルゴリズムにとって未知の場合, 信頼度の高いノイズ率の推定法の確立と分析がこの仕事の主な貢献である. 手法としては先行研究と同様にブール関数に対するフーリエ解析を用いている. フーリエ係数のうち ”低周波 ”だけの部分の自乗和とノイズ率の関係式を導出し, それに基づくノイズ率の推定法, そしてそれを用いる学習アルゴリズムの設計法を示した.

B05: ブール理論に基づく離散システムの構造解析と計算限界の研究

牧野 和久

大阪大学 大学院 基礎工学研究科
〒 560-8531 豊中市待兼山 1-3
makino@sys.es.osaka-u.ac.jp

摘要: 本文では，平成 16 年度の B05 班の研究活動に関係する成果を報告する．特に, 無向グラフの極大クリーク列挙問題に対する高速なアルゴリズムの開発について説明する．

キーワード: 計算効率，アルゴリズム，列挙

1 はじめに

社会システムや産業活動などに関連して現れる生産計画，環境計画，スケジューリング，最適投資などを始めとする重要な問題の多くは，離散構造を有するシステムの問題として捉えることができる．この離散構造を有するシステムの問題が答易に解けるか否かは, その対象となるシステムの構造に強く依存する. 比較的容易に解ける最適化問題の組合せ的, 代数的, あるいは, ブール関数的構造については, 例えばマトロイド構造や劣モジュラ構造というような離散的な構造が深く関係することが知られているが, それだけでは説明のつかない問題も数多い. また，最適化問題以外の問題，例えば，列挙問題などが，効率的に解けるために離散構造を解析することは極めて重要である．本研究班では，比較的容易に解ける問題の構造的性質をさらに詳細に吟味し, その構造を明らかにし, 効率的なアルゴリズムを設計するための統一的な指針を与えること，および，計算量理論を用いて計算量下界の提示などの計算限界を明らかにすることを試みる．

本研究班では，以上のような目的意識を持って, 主に理論的な研究に重点をおいて活動を続けて来た．以下の節では，本年度の成果は，以下に挙げられる．

1. 無向グラフの極大クリーク列挙問題に対する結果 [14]
2. ソース配置問題に対する結果 [18]
3. 複基多面体に関する結果 [8]
4. 無向木の分割問題に対する結果 [15]

本報告では，特に，1．2．について報告する．

2 無向グラフの極大クリーク列挙

無向グラフ $G = (V, E)$ に対して，$W \subseteq V$ 中の任意の 2 点 $v, w \in W$ が枝 $(v, w) \in E$ をもつとき，W はクリークと呼ばれる．さらに，任意の $W' \supsetneq W$ がクリークでないとき，極大クリークと呼ばれる．良く知られているように，最大クリーク（要素数が最大であるクリーク）を求める問題は，NP 困難であり [9]，極大クリークを 1 つ求めることは，多項式時間で可能である．極大クリークを全て求めるという，極大クリーク列挙問題は, 古くから盛んに行われている [5, 13, 12, 21]．また，この極大クリーク列挙問題は，データマイニング分野の閉集合列挙問題などと関連し，様々な応用をもっている (例えば，[11, 1, 2])．

1977 年に築山ら [21] は，最初の出力多項式（全多項式）時間である，$O(nm)$ 時間遅延アルゴリズムを開発した．ただし，$n = |V|$，$m = |E|$ とする．また，アルゴリズムの計算時間が入出力

長の多項式時間で押さえられるとき，そのアルゴリズムを出力多項式時間とよび，i 番目の出力してから $i+1$ 番目を出力するまでに必要な時間が入力長の多項式で押さえられているものを多項式時間遅延とよぶ．Lawler ら [12] はこの結果を一般のハイパーグラフの問題に拡張した (Eiter ら [7] はさらに一般化した）．千葉と西関 [5] は，$\mathrm{O}(a(G)m)$ 時間遅延アルゴリズムを開発し，高速化に成功している．ただし， $a(G)$ は，グラフ G のアーボレシティ（arboricity）であり，一般に，$m/(n-1) \leq a(G) \leq m^{1/2}$ が成立する．Johnson ら [13] は，すべての極大クリークを辞書式順に $\mathrm{O}(nm)$ 時間遅延で列挙するアルゴリズムを開発している．ただし，彼らのアルゴリズムは $\mathrm{O}(nN)$ 領域必要とする．ここで N は，極大クリーク数である．

本研究では，高速な行列積計算を用いることにより，$\mathrm{O}(M(n))$ 時間遅延でかつ，$\mathrm{O}(n^2)$ 領域必要とする極大クリーク列挙アルゴリズムを開発した．ただし，$M(n)$ とは，2 つの $n \times n$ 行列の積を計算するために必要な時間であり，現在のところ $\mathrm{O}(n^{2.376})$ 時間で可能なことが知られている [6], したがって，提案するアルゴリズムは密な，例えば，$m = \Omega(n^{1.689})$ であるグラフに対しては，最速である．

以下では，このアルゴリズムの概略を紹介する．

2.1 $\mathrm{O}(M(n))$ 時間遅延アルゴリズム

提案するアルゴリズムは，築山ら [21] と Johnson ら [13] が用いた逆探索（reverse search）に基づくものである．ここで，逆探索は，列挙問題を高速に解くために，Avis と福田 [4] によって提案された手法である．

$G = (V, E)$ を点集合 $V = \{v_1, \ldots, v_n\}$，枝集合 $E = \{e_1, \ldots, e_m\}$ である無向グラフとする． 点 $v \in V$ と点集合 $S \subseteq V$ の近傍を以下に与える．

$$\Gamma(v) = \{u \in V \mid (u, v) \in E\}$$

$$\Gamma(S) = \{u \in V \setminus S \mid (u, v) \in E \text{ for some } v \in S\}.$$

点集合 S と $i \in \{1, 2, \ldots, n\}$ に対して，

$$S_{\leq i} = S \cap \{v_1, \ldots, v_i\}.$$

2 つの点集合 X と Y に対して，$(X \setminus Y) \cup (Y \setminus X)$ 中の最小添字をもつ点が X に含まれるとき， X は，Y よりも辞書式に大きいと呼ぶ．また，クリーク K に対して，$C(K)$ を K を含む辞書式に最大の極大クリークと定義する．

逆探索は，直感的には，列挙しようする対象に親子関係を定義し，その関係をなぞることにより，高速に列挙を可能としている．本研究で扱った極大クリークに関しては以下のように親子関係を定義する．

K_0 を辞書式に最大である極大クリークとする．K_0 でない極大クリーク K に対して，$C(K_{\leq i-1}) \neq K$ を満たす最大の i における $C(K_{\leq i-1})$ をその親 $P(K)$ と定義する．また，そのような i を親インデクスと呼び，$i(K)$ と記す．$K \neq C(K_{\leq 0})$ なので，上記の $P(K)$ は定義可能であることが分かる．さらに，定義から $P(K)$ が K より辞書式に大きくなることから以下の補題を得る．

補題 1 極大クリーク上の親子関係が非巡回であり，K_0 を根とする内向木になる．

補題 1 中の内向木を列挙木と呼ぶ．[13, 21] のアルゴリズムは（見かけ上はかなり異なるが本質的に）この列挙木をなぞることにより，高速な極大クリーク列挙アルゴリズムを構成している．

定義からすぐに極大クリーク K からその親 $P(K)$ は線形時間で求められることが分かる．しかしながら，K からその子集合を求めることは，それほど簡単ではない．

極大クリーク K と $i \in \{1, 2, \ldots, n\}$ に対して，

$$K[i] \quad = \quad C\Big((K_{\leq i} \cap \Gamma(v_i)) \cup \{v_i\}\Big). \quad (2.10)$$

とする．

補題 2 K と K' をグラフ G の極大クリークとする．そのとき，K' が K の子であるために必要十分条件は，下記の 4 つの条件を満たす i に対して $K' = K[i]$ が成立することである．

(a) $v_i \notin K$.

(b) $i > i(K)$.

(c) $K[i]_{\leq i-1} = K_{\leq i} \cap \Gamma(v_i)$.

(d) $K_{\leq i} = C(K_{\leq i} \cap \Gamma(v_i))_{\leq i}$.

さらに，もし，i が (a) $\sim$ (d) を満たすならば，その i は，$K[i]$ の親インデクスとなる．

極大クリークの子集合を高速に求めるために，上記の補題 2 の条件 (c) と (d) を以下のように言い換える．

補題 3 K を G の極大クリークとする．このとき，i が条件 (c) をみたす必要十分条件は，下記の 3 つの条件を満たす j が存在しないことである．

(c-1) $j < i$.

(c-2) $v_j \notin K_{\leq i} \cap \Gamma(v_i)$.

(c-3) v_j が $K_{\leq i} \cap \Gamma(v_i) \cup \{v_i\}$ に属するすべての点と隣接している．

補題 4 K を G の極大クリークとする．このとき，i が条件 (d) をみたす必要十分条件は，下記の 4 つの条件を満たす j が存在しないことである．

(d-1) $j < i$.

(d-2) $v_j \notin K$.

(d-3) v_j が $K_{\leq j}$ に属するすべての点と隣接している．

(d-4) v_j が $K_{\leq i} \cap \Gamma(v_i)$ に属するすべての点と隣接している．

詳細は省略するが，本研究ではこの特徴付けを用いることにより，極大クリークのすべての子集合を $\mathrm{O}(M(n))$ 時間，$\mathrm{O}(n^2)$ 領域で計算可能なことを示し，以下の定理を得る．

定理 1 与えられた無向グラフ $G = (V, E)$ のすべての極大クリークを $\mathrm{O}(M(n))$ 時間遅延で，かつ，$\mathrm{O}(n^2)$ 領域で列挙できる．

3 ソース配置問題

点集合 V と枝集合 E をもつ無向グラフ G に容量関数 $u : E \to \mathbb{Z}_+$ を付与したものを無向ネットワークと呼び，$\mathcal{N} = (G = (V, E), u)$ と記す．ただし，$\mathbb{Z}_+$ は，非負整数の集合である．本論文では，この無向ネットワーク $\mathcal{N} = (G = (V, E), u)$，要求関数 $d : V \to \mathbb{Z}_+$，コスト関数 $c : V \to \mathbb{R}_+$ が与えられたとき，以下の条件を満たし，最小なコスト $(\sum_{v \in V} c(v))$ をもつ集合 $S \subseteq V$ を求めるというソース配置問題を考察する．ただし，$\mathbb{R}_+$ は，非負実数の集合である．

各点 $v \in V$ と S との間の最大フロー量 $\lambda(v, S)$ が要求値 $d(v)$ 以上である．

このソース配置問題は，例えば，マルチメディアネットワーク中にサービス要求量を指定した複数のクライアントが与えられたとき，その要求を満足しながら最小コストで（ミラー）サーバを配置するという問題に対応し，信頼度を考慮に入れた施設配置問題として近年盛んに研究されている (例えば，[3, 10, 16, 19, 20] など)．また，ネットワーク理論で有名な連結度増大問題とも深く関連している [17].

現在のところソース配置問題は，コスト関数が一様な場合 (要求関数は一様でなくてもよい) は，$\mathrm{O}(nM(n, m))$ 時間で解け，要求関数が一様な場合 (コスト関数は一様でなくてもよい) は，$\mathrm{O}(n(m + n \log n))$ 時間で解けることが示されている [3]．ここで，$M(n, m)$ を n 個の点，m 本の枝を持つ無向ネットワーク中の最大フローを求めるために要する時間である．また，コスト関数と要求関数ともに一般の場合は，ソース配置問題をナップサック問題へ帰着することで弱 NP 困難性が示されている．しかしながら，強 NP 困難であるか，あるいは，擬多項式時間アルゴリズムをもつかどうか未解決のまま残されており [3]，近似精度保証付きの近似アルゴリズムは，これまで開発されていない．

3.1 ソール配置問題の拡張

上記のソース配置問題では，コスト関数として施設の建設費用 (v における建設費用 $c(v)$) のみを扱っている．しかしながら，現実のコスト関数は建設費用に加え，供給量に依存する．従って，本研究では以下のように拡張したソース配置問題も考察する．

まず，無向ネットワーク $\mathcal{N} = (G = (V, E), u)$ を対称な有向ネットワーク $\hat{\mathcal{N}} = (\hat{G} = (V, \hat{E}), \hat{u})$ を見なす．ただし，$\hat{E} = \{(v, w), (w, v) \mid (v, w) \in E\}$ であり，任意の枝 $(v, w) \in E$ に対して，$\hat{u}(v, w) = \hat{u}(w, v) = u(v, w)$ と定義する．ここで，フロー $f : \hat{E} \to \mathbf{R}_+$ が以下の条件をみたすと

き，供給 $x : V \to \mathbf{R}_+$ に対して実行可能であると呼ぶ．

$$
\begin{aligned}
&(i)\ \ \partial f(v) \stackrel{\text{def}}{=} \sum_{(v,w)\in\hat{E}} f(v,w) - \sum_{(w,v)\in\hat{E}} f(w,v) \\
&\qquad\qquad \leq x(v) \qquad\qquad (v \in V) \\
&(ii)\ \ 0 \leq f(e) \leq \hat{u}(e) \qquad\qquad (e \in \hat{E})
\end{aligned}
$$

$\partial f(v)$ は，フロー f の v における境界と呼ばれ，v から出るフロー量の総和から入るフロー量の総和を引いたもので，(i) は，その境界が供給量 $x(v)$ 以下であることを示している．また，(ii) は，容量制約である．

我々は，無向ネットワーク $\mathcal{N} = (G = (V,E), u)$，要求関数 $d : V \to \mathbb{Z}_+$，コストを表す単調な凹関数 $c_v : \mathbf{R}_+ \to \mathbf{R}_+$ $(v \in V)$ が与えられたとき，各点 $v \in V$ への流入量 $(-\partial f(v))$ が少なくとも要求量 $d(v)$ 以上であり，かつ，最小なコスト $(\sum_{v\in V} c_v(x(v)))$ をもつ供給 $x \in \mathbb{R}_+^V$ を求める問題を考察する．ここで，c_v の単調凹性は，供給量 $x(v)$ が増せば，コストが増す（より正確には，減らない）が，割引率は上がることを意味しており，一つの自然な仮定である．

これまで要求量 $d(v)$ が一様な場合の拡張されたソース配置問題は考察されたきたが [17]．一般的な場合については考察されていない．

3.2 本研究での成果

本研究では，まず，上記の未解決として残されたソース配置問題の強 NP 困難性を証明する．

定理 2 ソース配置問題は，強 NP 困難である．

この証明においては，NP-困難問題として有名な集合被覆問題 [9] をソース配置問題に帰着させることで定理 2 を示す．

集合被覆問題とは，台集合 $U = \{1, 2, \ldots, p\}$ の部分集合族 $\mathcal{S} = \{S_1, S_2, \ldots, S_q\}$ が与えられたとき，U の要素をすべてカバーする最小サイズの $\mathcal{S}$ の部分族 $\mathcal{X}$(すなわち，$\bigcup_{S_i\in\mathcal{X}} S_i = U$ かつ $|\mathcal{X}|$ が最小) を求める問題である．この問題例 I からソース配置問題の問題例 J ($\mathcal{N} = (G, u)$，d，c) を以下のように構成する．

$$
\begin{aligned}
V &= \{t_1, t_2\} \cup \{s_1, \ldots, s_q\} \cup \{u_1, \ldots, u_p\} \\
E &= \{(t_1, s_i) \mid i = 1, \ldots, q\} \cup \{(s_i, u_j) \mid j \in S_i\} \\
&\qquad \cup \{(u_j, t_2) \mid j = 1, \ldots, p\}
\end{aligned}
$$

容量関数 u は，$u(t_1, s_i) = \ell_i$ $(i = 1, \ldots, q)$，$u(s_i, u_j) = 1$ $(j \in S_i)$，$u(u_j, t_2) = k_j - 1$ $(i = 1, \ldots, p)$ とする．ただし，$|S_i| = \ell_i$，$|\{i \mid S_i \ni j\}| = k_j$．また，要求関数 $d(v)$ は，$v = t_1, t_2$ のとき $\sum_i \ell_i$，それ以外は 0 とし，コスト関数 $c(v)$ は，$v = t_2$ のとき 0，$v \in \{s_1, \ldots s_q\}$ のとき 1，それ以外のとき $q + 1$ とする．

直感的には，点 s_i は集合 S_i に対応し，点 u_j は，U の要素 j に対応する．また，証明は紙面の都合上省略するが以下の性質が成り立つ．

補題 5 $\mathcal{X}$ が I の最適解となるための必要十分条件は，$Y = \{t_2\} \cup \{s_i \mid S_i \in \mathcal{X}\}$ が J の最適解となることである．

この補題より，定理 2 が示される．また，集合被覆問題の近似困難性らから下記の近似困難性も示すことができる．

定理 3 NP$\not\subseteq$ DTIME($N^{\log\log N}$) ならば，ある定数 $c > 0$ が存在して，ソース配置問題に対する多項式時間 $c \ln \sum_{v\in V} d(v)$-近似アルゴリズムは存在しない．

ここで，NP$\not\subseteq$ DTIME($N^{\log\log N}$) とは，任意の NP に属する問題が O($N^{\log\log N}$) 時間の決定性アルゴリズムをもたないことを意味し，多くの計算量理論の研究者によって信じられている．ただし，N を入力長とする．また，α-近似アルゴリズム A とは，近似比（すなわち，(A の出力する解の目的関数値)/(最適値)）が必ず α 以内である解を出力するアルゴリズムのことをいう．

一方肯定的な結果として，我々は欲張り法に基づく近似アルゴリズムを提案し，そのアルゴリズムが（オーダの意味で）最適であることを示す．

紙面の都合上証明は省略するが，以下に示す欲張り法に基づく近似アルゴリズムを構成する．

任意の $v \in V$ と $S \subseteq V$ に対して，以下のように関数 $\alpha : V \to \mathbb{R}_+$ と $\beta : V \to \mathbb{R}_+ \cup \{+\infty\}$ を定

義する．

$$\alpha_S(w) = \max\{d(w) - \lambda(w, S), 0\}$$
$$\beta_{(S,v)}(w) = \max\{\lambda(w, S \cup \{v\}) - \lambda(w, S), 0\}.$$

ただし，$\lambda(w, S)$ は，w-S 間の最大フロー量を表し，$w \in S$ のときは，$\lambda(w, S) = +\infty$ とする．また，$\infty - \infty = 0$ と仮定する．さらに，$\gamma_{(S,v)} = \min\{\alpha_S, \beta_{(S,v)}\}$，

$$g_S(v) = \frac{c(v)}{\sum_{w \in V} \gamma_{(S,v)}(w)} \qquad (2.11)$$

とする．

提案するアルゴリズムは，初期状態 $S = \emptyset$ から始まり，すべての $v \in V$ に対して g_S の分母が 0 とならない間，$g_S(v)$ を最小にする v を求め，$S := S \cup \{v\}$ と S を更新するものである．ここで，すべての $v \in V$ に対して g_S の分母が 0 のとき，S はソース配置問題の実行可能解であることに注意されたい．

詳しい証明は省略するが，ネットワーク $\mathcal{N}$ に対するカット関数の劣モジュラ性などを用いることで，上記のシンプルな欲張り法に基づくアルゴリズムが多項式時間であり，かつ，その近似率が $1 + \ln \sum_{v \in V} d(v)$ で押さえられることがわかる．

定理 4 ソース配置問題は，多項式時間で $1 + \ln \sum_{v \in V} d(v)$-近似可能である．

また，木構造ネットワークに対しては以下の結果を得る．

定理 5 与えられたネットワーク $\mathcal{N}$ が木構造であるならば，ソース配置問題は擬多項式時間アルゴリズムをもつ．

この定理と（木構造ネットワークを用いて得られた）弱 NP 困難性の結果 [3] は，木構造ネットワークにおけるソース配置問題の（P≠NP の下での）計算限界を示している．

拡張されたソース配置問題については，定義から明らかに本来のソース配置問題より簡単ではないので，定理 2，3 より，以下の否定的な結果を得る．

系 1 拡張されたソース配置問題は強 NP 困難である．また，NP$\not\subseteq$ DTIME($N^{\log \log N}$) ならば，ある定数 $c > 0$ が存在して，拡張されたソース配置問題に対する多項式時間 $c \ln \sum_{v \in V} d(v)$-近似アルゴリズムは存在しない．

肯定的な結果に関しては，我々は，定理 4 の近似アルゴリズムを一般化し，近似率の最適なアルゴリズムを得る．

定理 6 拡張されたソース配置問題は，多項式時間で $1 + \ln \sum_{v \in V} d(v)$-近似可能である．

また，上記の結果は，有向グラフのとき，また，辺連結度ばかりでなく，点連結度の場合に対しても適応可能であることを示すことができる．

参考文献

[1] R. Agrawal and R. Srikant, Fast algorithms for mining association rules in large databases, *Proc. VLDB '94,* pp. 487–499, 1994.

[2] R. Agrawal, H. Mannila, R. Srikant, H. Toivonen and A. I. Verkamo, Fast discovery of association rules, *In Advances in Knowledge Discovery and Data Mining,* MIT Press, pp. 307–328, 1996.

[3] K. Arata, S. Iwata, K. Makino and S. Fujishige, Locating sources to meet flow demands in undirected networks, *Journal of Algorithms*, 42 (2002) 54-68.

[4] D. Avis and K. Fukuda, Reverse search for enumeration, *Discrete App. Math.,* 65 (1996) 21–46.

[5] N. Chiba and T. Nishizeki, Arboricity and subgraph listing algorithms, *SIAM J. Comput.*, 14 (1985) 210-223.

[6] D. Coppersmith and S. Winograd, Matrix multiplication via arithmetic progression, *Journal of Symbolic Computation*, 9 (1990) 251–280.

[7] T. Eiter, G. Gottlob and K. Makino, New results on monotone dualization and generating hypergraph transversals, *SIAM J. Comput.*, 32 (2003) 514–537.

[8] S. Fujishige, K. Makino, T. Takabatake, and K. Kashiwabara, Polybasic polyhedra: Structure of polyhedra with edge vectors of support size at most 2, *Discrete Mathematics*, 280 (2004) 13-27.

[9] M. R. Garey and D. S. Johnson, *Computers and Intractability*, Freeman, New York, 1979.

[10] H. Ito and M. Yokoyama, Edge connectivity between nodes and node-subsets, *Networks*, 31 (1998) 157-164.

[11] S. R. Kumar, P. Raghavan, S. Rajagopalan, and A. Tomkins, Trawling the web for emerging cyber-communities, *Proc. the Eighth International World Wide Web Conference,* Toronto, Canada, 1999.

[12] E. L. Lawler, J. K. Lenstra and A. H. G. Rinnooy Kan, Generating all maximal independent sets, NP-hardness and polynomial-time algorithms, *SIAM J. Comput.*, 9 (1980) 558–565.

[13] D. S. Johnson, M. Yanakakis and C. H. Papadimitriou, On generating all maximal independent sets, *Info. Proc. Lett.*, 27 (1998) 119–123.

[14] K. Makino, T. Uno, New algorithms for enumerating all maximal cliques, *Algorithm Theory – SWAT 2004*, edited by T. Hagerup and J. Katajainen, Humlebaek (Denmark), Lecture Notes in Computer Science 3111 (2004) 260-272.

[15] S. Mamada, T. Uno, K. Makino, S. Fujishige, A tree partitioning problem arising from an evacuation problem in tree dynamic networks, *Journal of the Operations Research Society of Japan* 掲載決定.

[16] H. Nagamochi, T. Ishii and H. Ito, Minimum cost source location problem with vertex-connectivity requirements in digraphs, *Information Processing Letters*, 80 (2001) 287–294.

[17] 坂下麻里子, 牧野和久, 藤重悟, ラミナー被覆制約を持つ単調凹関数最小化問題, *FIT 2003*, 2 (2003) 9-10.

[18] 坂下麻里子, 牧野和久, 藤重悟, 無向ネットワーク中のソース配置問題に対する近似アルゴリズム, *FIT 2004*, 3 (2004) 5-6.

[19] H. Tamura, M. Sengoku, S. Shinoda and T. Abe, Some covering problems in location theory on flow networks, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E75-A (1992) 678-683.

[20] 田村, 菅原, 仙石, 篠田, 無向フローネットワークにおける総合被覆問題について, 電子情報通信学会論文誌, J81-A (1998) 863-869.

[21] S. Tsukiyama, M. Ide, H. Ariyoshi and I. Shirakawa, A new algorithm for generating all the maximal independent sets, *SIAM J. Comput.*, 6 (1977) 505–517.

研究業績一覧

学術論文

1. S. Fujishige, K. Makino, T. Takabatake, and K. Kashiwabara:
"Polybasic polyhedra: Structure of polyhedra with edge vectors of support size at most 2", Discrete Mathematics, 280, 13-27, 2004.
概要: In the present paper we introduce a generalized concept of base polyhedron. We consider a class of pointed convex polyhedra in $\mathbf{R}^V$ whose edge vectors have supports of size at most 2. We call such a convex polyhedron a polybasic polyhedron. The class of polybasic polyhedra includes ordinary base polyhedra, submodular/supermodular polyhedra, generalized polymatroids, bisubmodular polyhedra, polybasic zonotopes, boundary polyhedra of flows in generalized networks etc. We show that for a pointed polyhedron $P \subseteq \mathbf{R}^V$ the following three statements are equivalent:

(1) P is a polybasic polyhedron.
(2) Each face of P with a normal vector of the full support V is obtained from a base polyhedron by a reflection and scalings along axes.
(3) The support function of P is a submodular function on each orthant of $\mathbf{R}^V$.

This reveals the geometric structure of polybasic polyhedra and its relation to submodularity.

2. K. Makino, T. Uno:
"New algorithms for enumerating all maximal cliques", SWAT 2004, Lecture Notes in Computer Science, 3111, 260-272, 2004.
概要: In this paper, we consider the problems of generating all maximal (bipartite) cliques in a given (bipartite) graph $G = (V, E)$ with n vertices and m edges. We propose two algorithms for enumerating all maximal cliques. One runs with $\mathrm{O}(M(n))$ time delay and in $\mathrm{O}(n^2)$ space and the other runs with $\mathrm{O}(\Delta^4)$ time delay and in $\mathrm{O}(n+m)$ space, where Δ denotes the maximum degree of G, $M(n)$ denotes the time needed to multiply two $n \times n$ matrices, and the latter one requires $\mathrm{O}(nm)$ time as a preprocessing.

For a given bipartite graph G, we propose three algorithms for enumerating all maximal bipartite cliques. The first algorithm runs with $\mathrm{O}(M(n))$ time delay and in $\mathrm{O}(n^2)$ space, which immediately follows from the algorithm for the non-bipartite case. The second one runs with $\mathrm{O}(\Delta^3)$ time delay and in $\mathrm{O}(n+m)$ space, and the last one runs with $\mathrm{O}(\Delta^2)$ time delay and in $\mathrm{O}(n+m+N\Delta)$ space, where N denotes the number of all maximal bipartite cliques in G and both algorithms require $\mathrm{O}(nm)$ time as a preprocessing.

Our algorithms improve upon all the existing algorithms, when G is either dense or sparse. Furthermore, computational experiments show that our algorithms for sparse graphs have significantly good performance for graphs which are generated randomly and appear in real-world problems.

3. 坂下麻里子，牧野和久，藤重悟:
"無向ネットワーク中のソース配置問題に対する近似アルゴリズム", FIT 2004, 3, 5-6, 2004.
概要: 本研究では，無向ネットワーク中のソース配置問題が強 NP 困難であり，かつ近似不可能であることを示す．さらに，欲張り法に基づく最適な近似アルゴリズムを構成する

4. S. Mamada, T. Uno, K. Makino, S. Fujishige:
"A tree partitioning problem arising from an evacuation problem in tree dynamic networks", Journal of the Operations Research Society of Japan, （掲載予定）.
概要: In this paper, we present a first

polynomial time algorithm for the monotone min-max tree partitioning problem and show that the min-max tree partitioning problem is NP-hard if the cost function is not monotone, and that the min-sum tree partitioning problem is NP-hard even if the cost function is monotone. We also consider an evacuation problem in dynamic networks as an application of the tree partitioning problem. The evacuation problem is one of the basic studies on crisis management systems for evacuation guidance of residents against large-scale disasters. We restrict our attention to tree networks and consider flows such that all the supplies going through a common vertex are sent out through a single arc incident to it, since one of the ideal evacuation plans makes everyone to be evacuated fairly and without confusion.

研究会等

1. 間々田聡子, 宇野毅明，牧野和久, 藤重悟:
“木構造動的ネットワークにおける複数個の施設配置問題”, 日本応用数理学会研究部会連合発表会, 2005 年 3 月.
概要: 本研究では，各点に供給量 $b \in \mathbb{Z}_+^n$ をもつ木構造動的ネットワークと完了時間 θ が与えられたとき，θ 時間以内にすべての供給量を流し込むために必要な最小個数の点集合 W を求める問題を考察する．我々はこの施設配置問題に対する $O(n^2 \log^2 n)$ 時間アルゴリズムを開発する．

2. 坂下麻里子，牧野和久，藤重悟:
“フロー要求を持つ最小費用ソース配置問題”, 日本応用数理学会研究部会連合発表会, 2005 年 3 月.
概要: ソース配置問題とは，与えられたネットワークにおいて，フロー（連結度）に基づく制約条件の下で最小コストを与えるソース集合（配置）を求める問題である．我々はこのソース配置問題に対して以下の結果を得る．
1. 無向ネットワーク中の枝連結度に基づくソース配置問題の強 NP 困難性を示す．さらに近似困難性も示す.
2.(拡張された) ソース配置問題に対する近似アルゴリズムを開発する．このアルゴリズムは，枝連結度要求に対して最適な近似精度を与える．
3. 木構造ネットワークにおけるソース配置問題は，枝連結度要求のときは擬多項式時間で解け,（２種類の）点連結度要求のときは多項式時間で解けることを示す.
4. 無向ネットワーク中の一様な枝連結度要求を持つ拡張されたソース配置問題に対する $O(nm + n^2(q + \log n))$ 時間アルゴリズムを開発する．ただし，q は供給に対するコストを求めるために要する時間であり，コスト関数がオラクルで与えられるとき，上記のアルゴリズムは最適である．また，コスト関数が建設費と線形な運営費の和として記述できる場合はさらに高速に $O(n(m + n \log n))$ 時間で解け，より一般的なコスト関数に対しては計算困難であることを示す.

学会大会等

1. 牧野和久:
“単調ブール関数の双対化問題について”, 日本オペレーションズ・リサーチ学会秋季研究発表会, 182-183, 2004 年 11 月.

2. 間々田聡子, 宇野毅明，牧野和久, 藤重悟:
“木構造動的ネットワークにおける複数個の施設配置問題”, 日本オペレーションズリサーチ学会秋季研究発表会, 222-223, 2004 年 11 月.

3. 坂下麻里子，牧野和久，藤重悟:
“無向ネットワーク中のソース配置問題の強ＮＰ困難性とその近似アルゴリズム”, 日本オペレーションズ・リサーチ学会秋季研究発表会, 224-225, 2004 年 11 月.

B06: 暗号システムに対する実装攻撃の適用と限界に関する計算的研究

酒井 康行[1] †　田端 利宏[2] ‡　櫻井 幸一 ‡

† 三菱電機株式会社 情報技術総合研究所
〒 247-8501 神奈川県鎌倉市大船 5-1-1
ysakai@iss.isl.melco.co.jp

‡ 九州大学 大学院システム情報科学研究院
〒 812-8581 福岡県福岡市東区箱崎 6-10-1
{tabata, sakurai}@csce.kyushu-u.ac.jp

1 はじめに

楕円曲線暗号実装に対するサイドチャネル解析法を考察する．楕円曲線ドメインパラメータは，数学的安全条件を満たすように選ぶことは必須要件である．しかし，実際の情報セキュリティシステムへ楕円曲線暗号を適用するためには，数学的に安全であるだけでなく高い速度性能が得られるようなドメインパラメータを選択することが重要な要件となる．素体 $\mathbb{F}_p$ 上楕円曲線においては，定義体標数 p として特別な型，例えば一般化 Mersenne 素数を選ぶと p による剰余算を高速に行える [13]. National Institute of Standards and Technology (NIST) が推奨する 5 つの素体上楕円曲線は，一般化 Mersenne 素数を定義体標数としている [2].

一方，RSA 暗号実装では，法乗算に Montgomery 乗算法 [10] がよく用いられる．Montgomery 乗算は，法乗算への入力に依存した処理分岐が生じることから，タイミング攻撃が可能になることが知られている [7, 1, 11]．楕円曲線暗号においては，法 p を特殊な型にとって剰余算を高速化できることから，Montgomery 乗算ではなく，一般化 Mersenne 素数のような特殊な素数による専用剰余算アルゴリズムを用いることが多いと思われる．一般化 Mersenne 素数による剰余算の典型的な実装でも，後述するように Montgomery 乗算と同様に入力値に依存した処理分岐が生じる．

単純なバイナリ法のように，楕円点倍算において点加算と点 2 倍算とが秘密べき指数のビット値に依存して計算される時，単純電力解析 (Simple Power Analysis, SPA) によって秘密べき指数を導出することができる．SPA 対策の 1 つとして，異なる 2 点の加算と点 2 倍算とを同じ計算式で実行するというアプローチがある [3, 5, 6, 8]．これらの計算式は “unified code” と呼ばれる．Brier らは，Weierstrass 型楕円曲線 affine 座標系および射影座標系 ($(x, y) = (X/Z, Y/Z)$) において，入力の 2 点が異なる場合でも同じ場合でも，同じ手順で動作する点加算アルゴリズムを示した [3].

しかし Walter は，Montgomery 乗算を用いて Brier らの unified code を実装した場合，左バイナリ法による楕円点倍算は SPA に対して脆弱であることを示した [15]．この結果は Montgomery 乗算を用いた $\mathbb{F}_p$ 乗算であり，前述のように実際の情報セキュリティシステムで稼動している楕円曲線暗号は，p を一般化 Mersenne 素数など高速処理向きな楕円曲線ドメインパラメータによる専用の高速アルゴリズムが実装されていることが多いと思われる．

本稿では，より一般的な楕円曲線暗号実装である一般化 Mersenne 素数など高速処理向けな定義体標数を用いた剰余算実装に対する SPA を考察する．NIST 推奨曲線 [2] のような一般化 Mersenne 素数を用いた高速剰余算実装に対しても，unified code のように，楕円点加算と 2 倍算とを同じ処理手順で実装するだけでは SPA に対して安全ではないことを示す．特に NIST 推奨の素体上楕円曲線について，剰余算実装の SPA に対する脆弱性を考察する．5 つある推奨曲線のうち，192 ビットの曲線に用いられている素数 $p = 2^{192} - 2^{64} - 1$ による剰余算実装は，SPA に対してより脆弱になりやすいことを示す．

[1] 平成 16 年度 九州大学 大学院システム情報科学府博士（工学）の学位を取得

[2] 平成 17 年度 4 月 1 日付けで岡山大学 工学部 情報工学科（Email:tabata@it.okayama-u.ac.jp）

2 高速剰余算

RSA 暗号や (素体上) 楕円曲線暗号では，暗号や署名の演算は法演算の繰り返しである．除算命令は一般に演算時間がかかるため，除算命令無しで実装できる剰余算アルゴリズムを用いることが望ましい．Montgomery 乗算 [10] は，任意の法 n に対して除算命令を必要としないため，RSA 暗号ではよく用いられる．

一方，素体 $\mathbb{F}_p$ 上楕円曲線暗号では，p を法とする剰余算が行われる．p は公開パラメータであり，ランダムに選択する必要は無い．したがって，高速に演算可能な都合の良い p が選ばれる場合が多い[1]．

本章では，一般化 Mersenne 素数など，特別な型の素数を法とする高速剰余算アルゴリズムの概要を記述する．

2.1 一般化 Mersenne 素数

NIST による素体上推奨曲線 [2] は，一般化 Mersenne 素数と呼ばれる次のような素数 p をドメインパラメータとしている．

P-192: $p_{192} = 2^{192} - 2^{64} - 1$
P-224: $p_{224} = 2^{224} - 2^{96} + 1$
P-256: $p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
P-384: $p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$
P-521: $p_{521} = 2^{521} - 1$

p_{192}，p_{224}，p_{256}，p_{384}，p_{521} を法とする剰余算をそれぞれアルゴリズム 2.1，2.2，2.3，2.4，2.5 に示す [2, 4, 13]．

Algorithm 2.1 Fast reduction modulo $p_{192} = 2^{192} - 2^{64} - 1$

`Input` integer $c = (c_5, c_4, c_3, c_2, c_1, c_0)$, where each c_i is a 64-bit word, and $0 \le c < p_{192}^2$.
`Output` $c \bmod p_{192}$.

1. `Define 192-bit integers:`
   $s_0 = (c_2,\ c_1,\ c_0)$
   $s_1 = (\ 0,\ c_3,\ c_3)$
   $s_2 = (c_4,\ c_4,\ 0\ )$
   $s_3 = (c_5,\ c_5,\ c_5)$
2. `Return` $s_0 + s_1 + s_2 + s_3 \bmod p_{192}$

Algorithm 2.2 Fast reduction modulo $p_{224} = 2^{224} - 2^{96} + 1$

`Input` integer $c = (c_{13}, \ldots, c_1, c_0)$, where each c_i is a 32-bit word, and $0 \le c < p_{224}^2$.
`Output` $c \bmod p_{224}$.

1. `Define 224-bit integers:`
   $s_0 = (\ c_6,\ \ c_5,\ \ c_4,\ \ c_3,\ \ c_2,\ \ c_1,\ \ c_0\ )$
   $s_1 = (c_{10},\ c_9,\ \ c_8,\ \ c_7,\ \ 0,\ \ 0,\ \ 0\ )$
   $s_2 = (\ 0,\ \ c_{13},\ c_{12},\ c_{11},\ \ 0,\ \ 0,\ \ 0\ )$
   $s_3 = (c_{13},\ c_{12},\ c_{11},\ c_{10},\ \ c_9,\ \ c_8,\ \ c_7\ )$
   $s_4 = (\ 0,\ \ 0,\ \ 0,\ \ 0,\ \ c_{13},\ c_{12},\ c_{11})$
2. `Return` $s_0 + s_1 + s_2 - s_3 - s_4 \bmod p_{224}$

Algorithm 2.3 Fast reduction modulo $p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$

`Input` integer $c = (c_{15}, \ldots, c_1, c_0)$, where each c_i is a 32-bit word, and $0 \le c < p_{256}^2$.
`Output` $c \bmod p_{256}$.

1. `Define 256-bit integers:`
   $s_0 = (\ c_7,\ \ c_6,\ \ c_5,\ \ c_4,\ \ c_3,\ \ c_2,\ \ c_1,\ \ c_0\ )$
   $s_1 = (c_{15},\ c_{14},\ c_{13},\ c_{12},\ c_{11},\ \ 0,\ \ \ 0,\ \ 0\ )$
   $s_2 = (\ 0,\ \ c_{15},\ c_{14},\ c_{13},\ c_{12},\ \ 0,\ \ \ 0,\ \ 0\ )$
   $s_3 = (c_{15},\ c_{14},\ \ 0,\ \ \ 0,\ \ \ 0,\ \ c_{10},\ c_9,\ \ c_8\ )$
   $s_4 = (\ c_8,\ \ c_{13},\ c_{15},\ c_{14},\ c_{13},\ c_{11},\ c_{10},\ c_9\ )$
   $s_5 = (c_{10},\ c_8,\ \ \ 0,\ \ \ 0,\ \ \ 0,\ \ c_{13},\ c_{12},\ c_{11})$
   $s_6 = (c_{11},\ c_9,\ \ \ 0,\ \ \ 0,\ \ c_{15},\ c_{14},\ c_{13},\ c_{12})$
   $s_7 = (c_{12},\ \ 0,\ \ c_{10},\ c_9,\ \ c_8,\ \ c_{15},\ c_{14},\ c_{13})$
   $s_8 = (c_{13},\ \ 0,\ \ c_{11},\ c_{10},\ c_9,\ \ \ 0,\ \ c_{15},\ c_{14})$
2. `Return` $s_0 + 2s_1 + 2s_2 + s_3 + s_4 - s_5 - s_6 - s_7 - s_8 \bmod p_{256}$

Algorithm 2.4 Fast reduction modulo $p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$

`Input` integer $c = (c_{23}, \ldots, c_1, c_0)$, where each c_i is a 32-bit word, and $0 \le c < p_{384}^2$.
`Output` $c \bmod p_{384}$.

[1] RSA 暗号では，法 n はプライベート鍵であるランダムに生成された 2 つの素数 p，q の積であるため，高速演算に都合の良い n を選ぶことはできない．

1. Define 384-bit integers:
$s_0 = (c_{11}, c_{10}, c_9, c_8, c_7, c_6, c_5, c_4, c_3, c_2, c_1, c_0)$
$s_1 = (0, 0, 0, 0, 0, c_{23}, c_{22}, c_{21}, 0, 0, 0, 0)$
$s_2 = (c_{23}, c_{22}, c_{21}, c_{20}, c_{19}, c_{18}, c_{17}, c_{16}, c_{15}, c_{14}, c_{13}, c_{12})$
$s_3 = (c_{20}, c_{19}, c_{18}, c_{17}, c_{16}, c_{15}, c_{14}, c_{13}, c_{12}, c_{23}, c_{22}, c_{21})$
$s_4 = (c_{19}, c_{18}, c_{17}, c_{16}, c_{15}, c_{14}, c_{13}, c_{12}, c_{20}, 0, c_{23}, 0)$
$s_5 = (0, 0, 0, 0, c_{23}, c_{22}, c_{21}, c_{20}, 0, 0, 0, 0)$
$s_6 = (0, 0, 0, 0, 0, 0, c_{23}, c_{22}, c_{21}, 0, 0, c_{20})$
$s_7 = (c_{22}, c_{21}, c_{20}, c_{19}, c_{18}, c_{17}, c_{16}, c_{15}, c_{14}, c_{13}, c_{12}, c_{23})$
$s_8 = (0, 0, 0, 0, 0, 0, 0, c_{23}, c_{22}, c_{21}, c_{20}, 0)$
$s_9 = (0, 0, 0, 0, 0, 0, 0, c_{23}, c_{23}, 0, 0, 0)$
2. Return $s_0 + 2s_1 + s_2 + s_3 + s_4 + s_5 + s_6 - s_7 - s_8 - s_9 \bmod p_{384}$

Algorithm 2.5 Fast reduction modulo $p_{521} = 2^{521} - 1$

Input integer $c = (c_{1041}, \ldots, c_1, c_0)$, where $c_i \in \{0, 1\}$, and $0 \le c < p_{521}^2$.
Output $c \bmod p_{521}$.

1. Define 521-bit integers:
$s_0 = (c_{1041}, \ldots, c_{522}, c_{521})$
$s_1 = (c_{520}, \ldots, c_1, c_0)$
2. Return $s_0 + s_1 \bmod p_{521}$

2.2 Extra Reduction

アルゴリズム 2.1~2.5 は，各アルゴリズムのステップ 2 において入力に依存した条件付処理が生じる．例えば，p_{192} による剰余算アルゴリズム 2.1 のステップ 2 の典型的実装は次のようになる．

2.1. $t \leftarrow s_0 + s_1 + s_2 + s_3$
2.2. While $t \ge p_{192}$ do:
2.3. $t \leftarrow t - p_{192}$ (extra reduction)
2.4. end of while
2.5. Return t

アルゴリズム 2.1 の出力が p_{192} 未満であることを保証するために，ステップ 2.1 において s_0, s_1, s_2, s_3 を加算した結果 t が p_{192} 以上である場合，ステップ 2.3 において必要な回数 t から p_{192} を引く．この条件付引き算を “extra reduction” と呼ぶこととする．extra reduction が生じるかどうかは，剰余算への入力，すなわち法乗算への入力に依存して決まる．

入力に依存して生じる extra reduction に起因するサイドチャネル情報を利用した暗号解析法を第 4 章に示す．

2.3 その他の高速剰余算

Standards for Efficient Cryptography Group (SECG) が推奨している楕円曲線ドメインパラメータにも，素体 $\mathbb{F}_p$ 上楕円曲線の定義体標数 p として高速処理向けな型が選ばれている [12]．これらの素数には，NIST 推奨曲線のような一般化 Mersenne 素数や，$p = 2^t - c$ (c は小さい整数) という型の素数などが含まれている．

$p = 2^t - c$ 型素数に関しても，高速な剰余算アルゴリズムが知られている [9]．この剰余算アルゴリズムも，典型的な実装では，入力に依存した条件付処理，extra reduction，が生じる．したがって，第 4 章に示すサイドチャネル解析法は，$p = 2^t - c$ 型素数のための剰余算実装に対しても適用可能となる．

3 Unified Code

Weierstrass 型楕円曲線上の異なる 2 点の加算および点 2 倍算を，同じ演算手順で行える方法 “unified code” を Brier と Joye が提案した [3]．素体 $\mathbb{F}_p$ 上射影座標系，$(x, y) = (X/Z, Y/Z)$，におけるアルゴリズムを次に示す．

Algorithm 3.1 Unified point addition/doubling formula

Input $P_0 = (X_0, Y_0, Z_0), P_1 = (X_1, Y_1, Z_1) \in E(\mathbb{F}_p)$
Output $P_2 = P_0 + P_1 = (X_2, Y_2, Z_2) \in E(\mathbb{F}_p)$

1. $u_1 \leftarrow X_0 Z_1$, $u_2 \leftarrow X_1 Z_0$, $t \leftarrow u_1 + u_2$
2. $s_1 \leftarrow Y_0 Z_1$, $s_2 \leftarrow Y_1 Z_0$, $m \leftarrow s_1 + s_2$
3. $z \leftarrow Z_0 Z_2$, $f \leftarrow zm$, $l \leftarrow mf$, $g \leftarrow tl$
4. $r \leftarrow t^2 - u_1 u_2 + az^2$, $w \leftarrow r^2 - g$
5. $X_2 \leftarrow 2fw$
6. $Y_2 \leftarrow r(g - 2w) - l^2$
7. $Z_2 \leftarrow 2f^3$

8. Return $P_2 = (X_2, Y_2, Z_2)$

Unified code は，異なる 2 点の加算と点 2 倍算とを同じ手順で行うことにより，SPA に対する防御をねらったものである．しかし，第 4 章で述べるように，$\mathbb{F}_p$ 上乗算を Montgomery 乗算 [10] で実装した場合，SPA に対して脆弱になることを Walter が示した [15].

4 サイドチャネル解析

本章では，前章までに述べた一般化 Mersenne 素数による剰余算 (アルゴリズム 2.1~2.5) および unified code (アルゴリズム 3.1) を用いた実装に対するサイドチャネル解析を行う．楕円点倍算としてアルゴリズム 4.1 に示す左バイナリ法を用いる場合を考察する．

Algorithm 4.1 Left-to-right binary method of elliptic point multiplication

---

Input $G \in E(\mathbb{F}_p)$ and k, where $k = (k_{t-1}k_{t-2}\cdots k_0)$, $k_i \in \{0,1\}$ for $0 \le i \le t-2$, and $k_{t-1} = 1$

Output $R = kG$

1. $R \leftarrow G$
2. For i from $t-2$ down to 0 do:
3. $\quad R \leftarrow 2R$
4. $\quad$ If $k_i = 1$ then
5. $\quad\quad R \leftarrow R + G$
6. $\quad$ end if
7. end for
8. Return R

4.1 Extra Reduction の確率

まず，Extra reduction が生じる確率を実験的に評価する．評価において次を仮定する．

- 法乗算 $c \leftarrow a \times b \bmod p$ への 2 つの入力 a, b は一様であると仮定する．
- まず $a \times b$ を計算し，次にアルゴリズム 2.1~2.5 により剰余算を行う．
- アルゴリズム 2.1~2.5 ステップ 2 は，第 2.2 節に記述した手順で計算する．すなわち，まず全ての s_i について加減算を行い，その結果が p 以上の場合は，p 未満になるまで p を引く．

$c \leftarrow a \times b \bmod p$ の計算において，extra reduction が生じる確率は次の 3 つの場合で異なる．

- 法乗算への 2 つの入力 a，b が異なる場合
- $a = b$ の場合
- a と b の一方が定数の場合

一方が定数の場合，extra reduction の確率はその定数の値に依存する．

注意 4.1 楕円点倍算を左バイナリ法で行う場合は，点加算において常に決まった点 G を加算することになる *(アルゴリズム 4.1 ステップ 5)*．したがって，*unified code* の最初の *2* つのステップは，異なる *2* 点の加算の場合，法乗算は定数 *(*ベースポイントの x，y または $z(=1)$ 座標*)* との乗算である．

ランダム入力の場合

表 2.1 に法乗算への 2 つの入力整数が異なる場合，および 2 つの入力整数が同じ場合の extra reduction の確率を示す．ランダムに 100,000 個の整数ペア a, b $(0 \le a, b < p)$ を生成し，extra reduction が生じるかどうかを実験的に調べた．擬似乱数生成関数には，FIPS 186-2[2] に記載されている SHA-1 ベースのアルゴリズムを用いた．

P-192 と P-384 は他の曲線と比較して extra reduction が生じる確率が大きい．アルゴリズム 2.1~2.5 のステップ 2 からわかるように，P-192 の s_i は全て加算されるの対し，P-224, P-256, P-521 は加算される s_i が少ないことが原因である．また，P-384 も相対的に加算される s_i が多い．P-256 は，減算される s_i が多いため，extra reduction の確率が特に小さい．

ベースポイントの場合

表 2.2 に法乗算への 2 つの入力整数のうち一方が NIST 推奨曲線のベースポイント x 座標または

表 2.1: Probability of extra reduction with random inputs, where p is a recommended domain parameter.

Curve	$a \times b \bmod p$, $(a \neq b)$	$a \times a \bmod p$
P-192	0.69	0.73
P-224	0.30	0.27
P-256	0.11	0.20
P-384	0.65	0.69
P-521	0.25	0.33

y 座標の場合の extra reduction の確率を示す．前節と同様，ランダムに生成した 100,000 個の整数 a $(0 \leq a < p)$ に対して平均をとった．

表 2.2: Probability of extra reduction with fixed base point $G = (x_G, y_G, 1)$, where p and G are recommended domain parameters.

Curve	$a \times x_G \bmod p$	$a \times y_G \bmod p$
P-192	0.54	0.51
P-224	0.22	0.22
P-256	0.04	0.02
P-384	0.70	0.57
P-521	0.19	0.28

各曲線のベースポイントの x，y 座標値の上位桁のみを 16 進表記で次に示す．

P-192:

x_{192} =188da80eb03090f67cbf20eb43a18800f4f
...

y_{192} =07192b95ffc8da78631011ed6b24cdd573f
...

P-224:

x_{224}: b70e0cbd6bb4bf7f321390b94a03c1d356c
...

y_{224}: bd376388b5f723fb4c22dfe6cd4375a05a0
...

P-256:

x_{256}: 6b17d1f2e12c4247f8bce6e563a440f2770
...

y_{256}: 4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bc
...

P-384:

x_{384}: aa87ca22be8b05378eb1c71ef320ad746e1
...

y_{384}: 3617de4a96262c6f5d9e98bf9292dc29f8f
...

P-521:

x_{521}: 0c6858e06b70404e9cd9e3ecb662395b442
...

y_{521}: 11839296a789a3bc0045c8a5fb42c7d1bd9
...

表 2.2 からわかるように，P-192 はランダムな入力の場合 (表 2.1) よりも extra reduction の確率が小さい．ベースポイントの x 座標値，y 座標値ともに，上位桁の値が小さい (それぞれ 1 と 0) ことに起因する．

一方，P-224 は，ベースポイントの x 座標値の最上位桁と y 座標値の最上位桁は共に b であるが，extra reduction の確率は小さい．アルゴリズム 2.2 を見ると，剰余をとる整数 c の最上位ワード c_{13} は，和をとる s_0，s_1，s_2 の最上位ワードには含まれず，減じる s_3 の最上位ワードとなっている．したがって，c_{13} が大きいほど，すなわち法乗算への入力整数が大きいほど，extra reduction の確率は小さくなる．P-256，P-384，P-521 についても同様の現象を見ることができる．

なお，後述するように，ベースポイント座標値による法乗算において，extra reduction が生じる確率が大きいほど，SPA に対して脆弱となる．

4.2 攻撃法

Walter は条件付処理を持つ Montgomery 乗算実装に対する攻撃法を示した [15]．本節では，NIST 推奨素数による剰余算実装に対して同様の攻撃法を適用する．

楕円点倍算の実装に次の方法を用いる場合を考察する．

- **一般化 Mersenne 素数 p による剰余算:** 専用の高速アルゴリズム (アルゴリズム 2.1〜2.5 および第 2.2 節に記載の手順)
- **楕円点加算および点 2 倍算:** unified code(アルゴリズム 3.1)
- **楕円点倍算:** 左バイナリ法 (アルゴリズム 4.1)

また，攻撃者は次の能力を持つと仮定する．

- 実装されているアルゴリズムが前述のものであると知っている．
- 剰余算において extra reduction の有無を検出できる．

Unified code の実装 (アルゴリズム 3.1) は，入力の 2 点 P_0 および P_1 が同じ点 ($X_0 = X_1$，$Y_0 = Y_1$，$Z_0 = Z_1$) である場合，ステップ 1 における u_1 の計算と u_2 の計算は同じ計算となる．s_1，s_2 の計算 (ステップ 2) も同様である．したがって，u_1 と u_2 の計算のいずれか一方だけ，または s_1 と s_2 の計算のいずれか一方だけに extra reduction が生じた場合，点加算は同じ点に対するものとはなり得ず，必ず異なる 2 点に対するものだったことになる．このような場合，対応する秘密べき指数のビットは “1” と推定できる．

4.3 攻撃例

楕円曲線 P-192 に対する攻撃例を表 2.3 に示す．表 2.3 において，k は秘密べき指数の 2 進数表記である．ランダムに生成した 192 ビットの k のビットのうち，スペースの都合上，上位側のビットのみを示した．‘$\mathcal{AD}$’ は，左バイナリ法による楕円点倍算 (アルゴリズム 4.1) において，異なる 2 点の加算 $\mathcal{A}$ と同じ点の加算 (2 倍算)$\mathcal{D}$ のシーケンスを示す．シンボル ‘$*$’ は，u_1，u_2，s_1，s_2 の計算 (アルゴリズム 3.1) において，剰余算 (アルゴリズム 2.1) の際に extra reduction が生じたことを示す．シンボル ‘-’ は，extra reduction が生じなかったことを示す．

‘Difference’ の行には，u_1 と u_2 の一方だけに extra reduction が生じた場合，または s_1 と s_2 の一方だけに extra reduction が生じた場合にシンボル ‘Y’ を記述した．すなわち，‘Y’ の箇所では，unified code による点加算は，同じ点ではなく，異なる 2 点で行われたことになる．‘Recovered $\mathcal{AD}$’ は，サイドチャネル情報から推定できる $\mathcal{AD}$ のシーケンスを示している．推定可能な箇所にシンボル ‘Y’ を記述した．バイナリ法では，$\mathcal{A}$ の前後は必ず $\mathcal{D}$ であることに注意．

注意 4.2 この攻撃シミュレーションでは，*unified code* において，点 P_1 をアルゴリズム *4.1* における点 G とした．加算する固定点 G は署名生成などではベースポイントであり，通常は常に $Z_1 = 1$ である．したがって u_1 および s_1 の計算時に *extra reduction* は生じない．

4.4 防御法

Extra reduction の有無に起因する消費電力の違い，処理時間差などを観測できなくすることが本稿で述べた攻撃法に対する防御となる．

また，剰余算のアルゴリズムを考慮して，ベースポイントの座標値を適切に選択すれば，extra reduction の確率を減らすことができる．

5 まとめ

素体 $\mathbb{F}_p$ 上楕円曲線暗号実装において，剰余算に関するサイドチャネル情報漏洩を考察した．定義体標数 p には，通常，NIST 推奨曲線のように一般化 Mersenne 素数など高速に法乗算が行える素数が選ばれる．その素数専用の高速剰余算の典型的実装では，Montgomery 乗算の場合のように，入力に依存した extra reduction が生じる．Extra reduction の有無は，サイドチャネル攻撃の原因となり得る．Brier らの unified code は，異なる 2 点の加算と同じ点どうしの加算 (2 倍算) を，有限体演算レベルで同じ手順で行えるものであった．しかし，Montgomery 乗算における extra reduction の有無を攻撃者が検出できる場合，unified code のアプローチは SPA に対して脆弱となることが Walter によって指摘されていた [15]．本稿では，多くの楕円曲線暗号で用いられる一般化 Mersenne 素数による剰余算実装に対しても SPA が可能となることを示した．また，NIST による素体上推奨曲線のうち，192 ビットの曲線に用いられている素数による剰余算実装は，SPA に対して脆弱になりやすいことを示した．

参考文献

[1] J.F. Dhem, F. Koeune, P.A. Leroux, P. Mestré and J.-J. Quisquater, “A practical implementation of the timing attack,” CARDIS 1998, LNCS 1820, pp.175–190, Springer-Verlag, 1998.

表 2.3: An Attack on P-192

k	1001 01 1 001 001 001 01 1 01 1 01 1 1 1 1 0001 01 1 01 001 01 01 001 0 ...
$\mathcal{AD}$	DDDADDADADDDADDDADDDADDADADDADADDADADADADADDDDADDADADDADDDADDADDADDDAD ...
u_1	-*-----*-*-*-*-*-**--**-*-**---**-*-*-----****--*---**-***-*--**-***-* ...
u_2	-*----**-*-***-*-**--****-**--*****-*-----****--*--*********-********* ...
s_1	-**----*-**--***-**--*--*--*-*-**-*---*---***--*--*-**--*-----*--***-* ...
s_2	-**---*****-*******--*--*--********---*--****-**--*-**--*-*--**-****-* ...
Difference	------Y-Y---Y---Y------Y----Y-Y--Y-------Y----Y----Y--Y---Y--Y--Y---Y- ...
Recovered $\mathcal{AD}$	-----YYYYY-YYY-YYY----YYY--YYYYYYYY-----YYY--YYY--YYYYYY-YYYYYYYYY-YYY ...

[2] "Digital signature standard (DSS)," FIPS PUB 186-2, U.S. National Institute of Standards and Technology, 2000.

[3] E. Brier and M. Joye, "Weierstrass elliptic curves and side-channel attacks," Public Key Cryptography – PKC 2002, LNCS 2274, pp.335–345, Springer-Verlag, 2002.

[4] M. Brown, D. Hankerson, J. Lopez and A. Menezes, "Software implementation of the NIST elliptic curves over prime fields," Technical Report CORR 2000-56, University of Waterloo, 2000.

[5] C. Gebotys and R. Gebotys, "Secure elliptic curve implementations: an analysis of resistance to power-attacks in a DSP processor," Cryptographic Hardware and Embedded Systems – CHES 2002, LNCS 2523, pp.114–128, Springer-Verlag, 2002.

[6] M. Joye and J.-J. Quisquater, "Hessian elliptic curves and side channel attacks," Cryptographic Hardware and Embedded Systems – CHES 2001, LNCS 2162, pp.402–410, Springer-Verlag, 2001.

[7] P.C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," Advances in Cryptology – CRYPTO '96, LNCS 1109, pp.104–113, Springer-Verlag, 1996.

[8] P.-Y. Liardet and N.P. Smart, "Preventing SPA/DPA in ECC systems using the Jacobi form," Cryptographic Hardware and Embedded Systems – CHES 2001, LNCS 2162, pp.391–401, Springer-Verlag, 2001.

[9] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1966.

[10] P.L. Montgomery, "Modular multiplication without trial division," Mathematics of Computation, vol. 44, no. 170, pp.519–521, 1885.

[11] W. Schindler, "A timing attack against RSA with the Chinese Remainder Theorem," Cryptographic Hardware and Embedded Systems – CHES 2000, LNCS 1965, pp.109–124, Springer-Verlag, 2000.

[12] Certicom, "Standard for efficient cryptography, SEC2: Recommended elliptic domain parameters," 2000.

[13] J.A. Solinas, "Generalized Mersenne numbers," Technical Report CORR 99-39, University of Waterloo, 1999.

[14] C.D. Walter, "Sliding windows succumbs to Big Mac Attack," Cryptographic Hardware and Embedded System – CHES 2001, LNCS 2162, pp.286–299, Springer-Verlag, 2001.

[15] C.D. Walter, "Simple power analysis of unified code for ECC double and add," Cryptographic Hardware and Embedded System – CHES 2004, LNCS 3156, pp.191–204, Springer-Verlag, 2004.

研究業績一覧

学術論文

1. Yasuyuki Sakai, Kouichi Sakurai:
"On the Vulnerability of Exponent Recod-

ings for the Exponentiation against Side Channel Attacks", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E88A, No.1, 154-160, 2005年1月.
概要: In this paper we propose a new side channel attack, where exponent recodings for public key cryptosystems such as RSA and ECDSA are considered. The known side channel attacks and countermeasures for public key cryptosystems were against the main stage (square and multiply stage) of the modular exponentiation (or the point multiplication on an elliptic curve). We have many algorithms which achieve fast computation of exponentiations. When we compute an exponentiation, the exponent recoding has to be carried out before the main stage. There are some exponent recoding algorithms including conditional branches, in which instructions depend on the given exponent value. Consequently exponent recoding can constitute an information channel, providing the attacker with valuable information on the secret exponent. In this paper we show new algorithms of attack on exponent recoding. The proposed algorithms can recover the secret exponent, when the width-w NAF and the unsigned/signed fractional window representation are used.

2. Yasuyuki Sakai, Kouichi Sakurai:
"Timing Attacks against a Parallelized RSA Implementation", IPSJ, Vol. 45, No.8, 1813-1822, 2004年8月.
概要: We discuss timing attacks against RSA using the parallel modular exponentiation. We describe a parallel algorithm for the modular exponentiation $y \equiv x^d \bmod n$. Then timing attacks against the parallel implementation are demonstrated. When we have two processors, which perform the modular exponentiation, an exponent d is scattered into two partial exponents $d^{(0)}$ and $d^{(1)}$, where $d^{(0)}$ and $d^{(1)}$ are derived by bitwise AND operation from d such that $d^{(0)} = d \wedge (0101\cdots01)_2$ and $d^{(1)} = d \wedge (1010\cdots10)_2$. Two partial modular exponentiations $y_0 \equiv x^{d^{(0)}} \bmod n$ and $y_1 \equiv x^{d^{(1)}} \bmod n$ are performed in parallel using two processors. Then we can obtain y by computing $y \equiv y_0 y_1 \bmod n$. In general, the hamming weights of $d^{(0)}$ and $d^{(1)}$ are smaller than that of d. Thus a fast computation of the modular exponentiation $y \equiv x^d \bmod n$ can be achieved. We describe a timing attack against RSA with and without the Chinese Remainder Theorem (CRT) using the parallel modular exponentiation. Both the secret exponents $d_p = d \bmod p-1$ and $d_q = d \bmod q-1$, where $n = pq$, are scattered into two partial exponents, respectively. We show that timing attacks are still applicable to that case.

3. Yasuyuki Sakai, Kouichi Sakurai:
"A New Attack with Side Channel Leakage during Exponent Recoding Computations", Cryptographic Hardware and Embedded Systems – CHES 2004, Springer LNCS No. 3156, 298-311, 2004年8月.
概要: In this paper we propose a new side channel attack, where exponent recodings for public key cryptosystems such as RSA and ECDSA are considered. The known side channel attacks and countermeasures for public key cryptosystems were against the main stage (square and multiply stage) of the modular exponentiation (or the point multiplication on an elliptic curve). We have many algorithms which achieve fast computation of exponentiations. When we compute an exponentiation, the exponent recoding has to be carried out before the main stage. There are some exponent recoding algorithms including conditional branches, in which instructions depend on the given exponent value. Consequently exponent recoding can constitute

an information channel, providing the attacker with valuable information on the secret exponent. In this paper we show new algorithms of attack on exponent recoding. The proposed algorithms can recover the secret exponent, when the width-w NAF and the unsigned/signed fractional window representation are used.

4. Dong-Guk Han, Tetsuya Izu, Jongin Lim, and Kouichi Sakurai:
"Side Channel Cryptanalysis on XTR Public Key Cryptosystem", IEICE Trans. Fundamentals, Special Section on Discrete Mathematics and Its Applications 2005, .
概要: The XTR public key cryptosystem was introduced in 2000. XTR is suitable for a variety of environments including low-end smart cards, and is regarded as an excellent alternative to RSA and ECC. Moreover, it is remarked that XTR single exponentiation (XTR-SE) is less susceptible than usual exponentiation routines to environmental attacks such as the timing attack and the differential power analysis (DPA). This paper investigates the security of side channel attack (SCA) on XTR. In this paper, we show the immunity of XTR-SE against the simple power analysis if the order of the computation of XTR-SE is carefully considered. In addition, we show that XTR-SE is vulnerable to the data-bit DPA, the address-bit DPA, the doubling attack, the modified refined power analysis, and the modified zero-value attack. Moreover, we propose some countermeasures against these attacks. We also show experimental results of the efficiency of the countermeasures. From our implementation results, if we compare XTR with ECC with countermeasures against "SCAs", we think XTR is as suitable to smart cards as ECC.

5. Dong-Guk Han, Jongin Lim, and Kouichi Sakurai:
"On security of XTR public key cryptosystems against Side Channel Attacks", Proceedings of Information Security and Privacy (ACISP 2004), LNCS 3108, 454-465, 2004年7月.
概要: The XTR public key system was introduced at Crypto 2000. It is regarded that XTR is suitable for a variety of environments, including low-end smart cards, and XTR is the excellent alternative to either RSA or ECC. Previous works remarked that XTR single exponentiation (XTR-SE) is less susceptible than usual exponentiation routines to environmental attacks such as timing attacks and Differential Power Analysis (DPA). In this paper, however, we investigate the security of side channel attack (SCA) on XTR. This paper shows that XTR-SE is immune against simple power analysis under assumption that the order of the computation of XTR-SE is carefully considered. However, we show that XTR-SE is vulnerable to Data-bit DPA, Address-bit DPA, and doubling attack. Moreover, we propose countermeasures that prevent the proposed attacks. As the proposed countermeasure against doubling attack is very inefficient, a good countermeasure against doubling attack is actually necessary to maintain the advantage of efficiency of XTR.

6. Dong-Guk Han, Tetsuya Izu, Jongin Lim, and Kouichi Sakurai:
"Modified Power-Analysis Attacks on XTR and An Efficient Countermeasure", Information and Communications Security (ICICS 2004), LNCS 3269, 305-317, 2004年11月.
概要: Han et al. presented a nice overview of some side channel attacks (SCA), and some classical countermeasures. However, their proposed countermeasures against SCA are so inefficient that the efficiency of XTR with SCA countermeasures is at least

129 times slower than that of XTR without them. Thus they remained the construction of the efficient countermeasures against SCA as an open question. In this paper, we show that XTR can be also attacked by the modified refined power analysis (MRPA) and the modified zero-value attack (MZVA). To show validity of MRPA and MZVA on XTR, we give some numerical data of them. We propose a novel efficient countermeasure (XTR-RSE) against "SCAs": SPA, Data-bit DPA, Address-bit DPA, Doubling attack, MRPA, and MZVA. We show that XTR-RSE itself without other countermeasures is secure against all "SCAs". From our implementation results, if we compare XTR with ECC with countermeasures against "SCAs", we think XTR is as suitable to smart-cards as ECC due to the efficiency of the proposed XTR-RSE.

7. Dong-Guk Han, Tetsuya Izu, Jongin Lim, and Kouichi Sakurai:
"Side Channel Attacks on XTR and An Efficient Countermeasure", Technical Report of IEICE,ISEC2004-56, Vol. 104 No.200, 103-110, 2004年7月.
概要: Han et al. presented a nice overview of some side channel attacks (SCA) against XTR, and some classical countermeasures. However, their proposed countermeasures against SCA are so inefficient that the efficiency of XTR with SCA countermeasures is at least 129 times slower than that of XTR without them. Thus they remained the construction of the efficient countermeasures against SCA as an open question. In this paper, we show that XTR can be also attacked by the modified refined power analysis (MRPA) and the modified zero-value attack (MZVA). To show validity of MRPA and MZVA on XTR, we give some numerical data of them. We propose a novel efficient countermeasure against "SCAs": SPA, Data-bit DPA, Address-bit DPA, Doubling attack , MRPA, and MZVA. The proposed countermeasure, that is XTR-RSE, uses the exponent splitting method with a random number. We show that XTR-RSE itself without other countermeasures is secure against all "SCAs". From our implementation results, if we compare XTR with ECC with countermeasures against "SCAs", we think XTR is more suitable to smart-cards than ECC due to the efficiency of the proposed XTR-RSE.

研究会等

1. Yasuyuki Sakai, Kouichi Sakurai:
"Side Channel Analysis on Modular Reduction for Elliptic Curve Cryptosystems", 2005 Symposium on Cryptography and Information Security (SCIS2005), 2005年1月.
概要: We discuss side channel leakage on modular reduction with generalized Mersenne prime. FIPS 186-2 has 5 recommended prime fields. All the recommended elliptic curve domain parameters over $\mathbb{F}_p$ use special form primes, such as generalized Mersenne primes, for their field order p. These special form primes facilitate especially efficient implementation. A typical implementation of efficient modular reduction with such primes includes conditional subtractions. A conditional subtraction in modular reduction is assumed to give side channel leakage. Several authors have produced unified code for elliptic point addition and doubling in order to avoid a simple power analysis (SPA). However, Walter showed that SPA still be possible if Montgomery multiplication with conditional subtraction is implemented for the unified code. In this paper we show SPA on the fast modular reduction with generalized Mersenne prime, combining with the unified

code for elliptic point operations. A practical cryptosystem based on an elliptic curve is implemented with special form primes to achieve fast implementation. Our results indicate that even if the unified codes are implemented for point operations, underlying field operations should be implemented in constant time. The unified approach in itself can not be a countermeasure for side channel attacks.

2. Dong-Guk Han, Dongjin Yang, Jongin Lim, and Kouichi Sakurai:
"DPA on Hybrid XTR Single Exponentiation", 2005 Symposium on Cryptography and Information Security (SCIS2005), Vol.II, 601-606, 2005 年 1 月.
概要: Han et al. presented a nice overview of some side channel attacks, and some classical countermeasures. They considered SPA, DPA, Doubling Attack, Refined Power analysis, and Zero value attack on XTR single exponentiation. Previous works applied SPA to XTR-SE using simultaneous XTR double exponentiation (Hybrid XTR-SE). Chung-Hasan showed it takes $2^{0.625*k}$ tries for an attacker until he/she correctly finds the secret value in Hybrid XTR-SE where k is a bit-length of secret value. Page-Stam showed it requires $2^{0.55*k}$ tries. But these results are far worse than well-known square-root type algorithms (Baby-Step-Giant-Step or Pollards' Rho methods). From the above related results for XTR with side channel attack, there are many research results for XTR-SE with several side channel attacks, but *no actual attacks* on Hybrid XTR-SE have been proposed so far. In this paper we propose enhancing differential power analysis on Hybrid XTR-SE.

C01: グラフ描画アルゴリズムとそのWeb情報検索への応用

西関 隆夫　周 暁　Md. Saidur Rahman　三浦 一之　浅野 泰仁

東北大学 大学院 情報学研究科
〒 980-8579 仙台市青葉区荒巻字青葉 6-6-05
{nishi,zhou,saidur}@ecei.tohoku.ac.jp, {miura,asano}@nishizeki.ecei.tohoku.ac.jp

1　はじめに

本研究課題の研究成果概要は以下の通りである.

(1) Rahman, 西関らによってこれまでに得られた成果を中心にして，グラフ描画の理論とアルゴリズムを集大成して，英文の成書”Planar Graph Drawing”を執筆し，World Scientific 社から Lecture Notes Series on Computing Vol. 12 として出版した.

(2) 購入したパーソナルコンピュータを用いて，各面の面積が指定された平面グラフを，外面が長方形，内面が水平・垂直線分のみからなる八角形に描画するアルゴリズムを実装し，その実用性を検証した．また，VLSI レイアウトにこのアルゴリズムを適用した場合，対応する VLSI を設計しやすくするためには八角形ができるだけ幅の細い部分を持たないようにした方が良いが，様々なヒューリスティクスを用いて，これを可能にした.

(3) 平面グラフの格子凸描画において，別個に研究されてきた標準分解，リアライザ，シュナイダーラベリング，順序つき全域木がすべて同等であることを証明した.

(4) 直並列グラフの折れ曲がりなし直交描画の線形時間アルゴリズムを開発した.

(5) 内部三角化平面グラフが開 RI 描画 (グラフの各辺を対角線とする長方形の内部に他の点がない描画) をもつための必要十分条件と，線形時間描画アルゴリズムを与えた.

(6) ウェブ文書データを解析し，申請者らが提案したフィルタと呼ばれる手法によって，サイトのデータを抽出した．また，このデータから構築されたウェブグラフ (ページを点とする) とサイト間グラフ (サイトを点とする) 両方の上で，著名な情報検索手法である max-flow based method による実験を繰り返し，サイト間グラフがこの手法にきわめて有効であることを示した．さらに，サイト間グラフのリンク，サイト内のリンクを描画してコミュニティとリンクの関係をわかりやすく図示するためのツールを上述のグラフ描画アルゴリズムを応用して開発した.

以下，各章において，順に (2)–(6) の各成果について述べる.

2　面積指定 8 角形描画

平面グラフ G の各点を点として描き，G の各辺を水平あるいは垂直線分の列として描き，G の任意の 2 辺は共通の端点以外では交差しないように描いた描画を G の**直交描画**という．直交描画では，G の各面は軸平行多角形で描画される．直交描画はデータベースや VLSI 設計などに様々な応用をもつ ([RNN02] 参照).

G の直交描画で，G の各内面が指定された面積を持ち，しかも外面は各内面に指定された面積の合計と等しい面積の長方形として描かれる描画を**面積指定直交描画**という．G の面積指定直交描画で，各内面が高々8 つの角しかもたない軸平行多角形で描画されるものを，G の**面積指定 8 角形描画**という．Rahman, 三浦, 西関は G が “**良スライスグラフ**“ と呼ばれるグラフのクラスならば，面積指定 8 角形描画を持つということを示した．面積指定 8 角形描画アルゴリズムでは入力は，各面の面積が指定された良スライスグラフ G と，G に対応する**良スライス木**と呼ばれる木であり，出力

は面積指定 8 角形描画である（図 2.1 参照）.

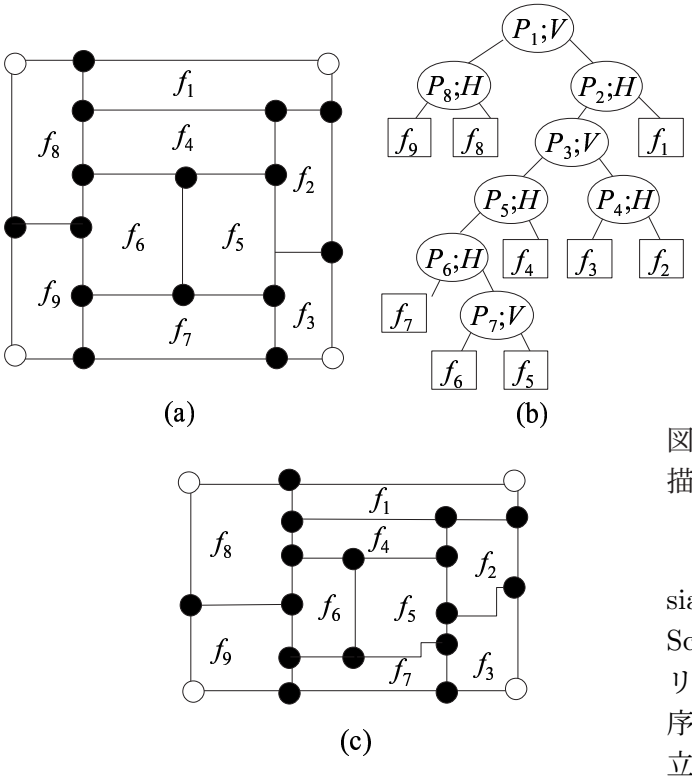


図 2.1: (a) 良スライスグラフ G，(b) 良スライス木 T，(c) 面積指定 8 角形描画.

本研究では, 購入したパーソナルコンピュータを用いて，面積指定 8 角形描画アルゴリズムを実装し，その実用性を検証した. また，VLSI レイアウトにこのアルゴリズムを適用した場合，対応する VLSI を設計しやすくするためには八角形ができるだけ幅の細い部分 (図 2.1 (c) における，面 f_2, f_3, f_5, f_7 のように折れ曲がりがある箇所) を持たないようにした方が良いが，様々なヒューリスティクスを用いて，これを可能にした.

3　平面グラフの格子凸描画

外面を三角形とする格子凸描画とは，図 2.2 のようなものである.

2 連結平面グラフが外面を三角形とする格子凸描画をもつための条件としては，Chrobak, Kant によって提案された標準分解，Battista, Tamassia，Vismara によって提案されたリアライザ, Schnyder によって提案されたシュナイダーラベリング，Chiang, Lin, Lu によって提案された順序つき全域木がある．しかし，これらの概念は独立して研究されたもので，一部が等価であることは知られていたものの，すべてが等価であるかどうかは知られていなかった．われわれは本研究において，上記のすべての概念が等価，すなわち与えられたグラフが上記のいずれかをもてば上記のすべてをもつことを示した.

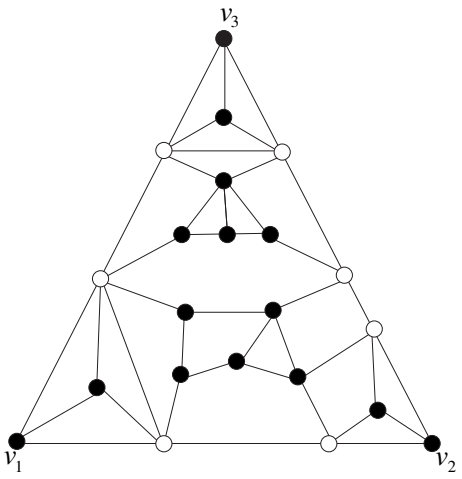


図 2.2: 平面グラフの外面を三角形とする格子凸描画

以下に，参考として，標準分解がどのようなものか記す.

3.1　標準分解

任意の 3 連結平面グラフは標準分解をもつ．標準分解とは，グラフの点集合の分割 $\Pi = (V_1, V_2, \cdots, V_h)$ で，以下の性質を満たすものである．なお，グラフの点集合 $V = \{u_1, u_2, \cdots, u_n\}$ のうち 3 点 u_1, u_2, u_n が時計回りに外周上に配置されるものとする．分割された点集合のひとつ V_k によって誘導される部分グラフを G_k, $V_{k+1} \bigcup V_{k+2} \bigcup \cdots \bigcup V_h$ によって誘導される部分グラフを $\overline{G_k}$ とする.

(cd1) V_1 が 外辺 (u_1, u_2) を含んでいる内面の境界上のすべての点からなり，かつ $V_h = \{u_n\}$ である.

(cd2) $1 \leq k \leq h$ の各 k について，G_k は内部 3 連結である．

(cd3) $2 \leq k \leq h$ の各 k について，V_k のすべての点は G_k の外点である．さらに，

(a) もし $|V_k| = 1$ ならば，その唯一の点 w は G_{k-1} 上に 2 つ以上の隣接点をもち，$k < h$ のときは $\overline{G_k}$ 上に 1 つ以上の隣接点をもつ．

(b) もし $|V_k| \geq 2$ ならば，V_k の点は G_k の描画上で連続して現れる．さらにその最初の点と最後の点は，G_{k-1} 上の点ひとつずつと隣接する．他の点は G_{k-1} に隣接点をもたない．また，各点は $\overline{G_k}$ 上に 1 つ以上の隣接点をもつ．

図 2.2 で与えられるグラフの標準分解の例を図 2.3 に示す．

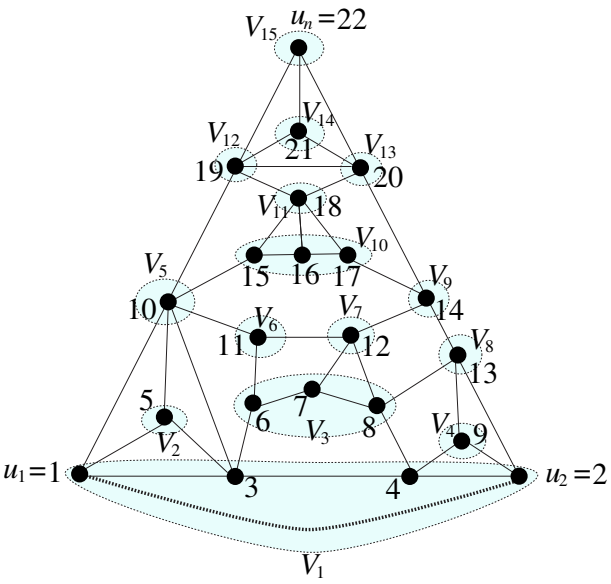


図 2.3: 図. 2.2 のグラフの標準分解 $\Pi = (V_1, V_2, \cdots, V_{15})$.

4 直並列グラフの折れ曲がりなし直交描画

グラフ G が (始点 v_{in} と終点 v_{out} をもつ) 直並列グラフであるとは，$G = (V, E)$ が 1 本の辺によってつながっている点のペア 1 つからなる (Fig. 2.4(a) 参照) か，あるいは 2 つの直並列グラフ $G_i = (V_i, E_i), i = 1, 2$ (始点はそれぞれ $v_{in,i}$, 終点はそれぞれ $v_{out,i}$) を $V = V_1 \cup V_2, E = E_1 \cup E_2$ かつ下の (1), (2) どちらかを満たすようにつなげたものになっている

(1) $v_{in} = v_{in,1}$, $v_{out,1} = v_{in,2}$, $v_{out2,} = v_{out}$ (Fig. 2.4(b) 参照),

(2) $v_{in} = v_{in,1} = v_{in,2}$, $v_{out} = v_{out,1} = v_{out,2}$ (Fig. 2.4(c 参照).

かどちらかである．Fig. 2.4(d) のグラフは，直並列グラフの一例である．

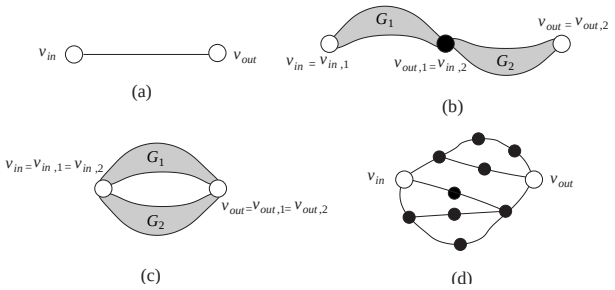


図 2.4: (a) もっとも単純な直並列グラフ, (b) 直列結合, (c) 並列結合 (d) 直並列グラフ.

直並列グラフは平面的グラフでもある．平面的グラフとは，平面に辺を交わることなく描画可能なグラフであり，その描画は通常何通りもある．平面グラフとは，平面的グラフの点と辺で囲まれる面の位置関係をひとつに定めたものである．したがって，平面的グラフより可能な描画は少ない．平面的グラフの折れ曲がりなし直交描画とは辺を水平線分ないし垂直線分で描いた描画である．Rahman, 西関らは以前，最大次数 3 以下の平面グラフが折れ曲がりなし直交描画をもつための必要十分条件と，その描画を求めるための線形時間アルゴリズムを与えた．しかし，最大次数 3 以下の平面的グラフに関しては，Di Battista らの計算量 $O(n^5 \log n)$ (n はグラフの点数) で折れ曲がりなし直交描画をもつかどうか判定できるという結果しか知られていない．

今回，われわれは最大次数 3 以下の直並列グラフが折れ曲がりなし直交描画をもつかどうか線形時間で判定できるアルゴリズムを与えた．

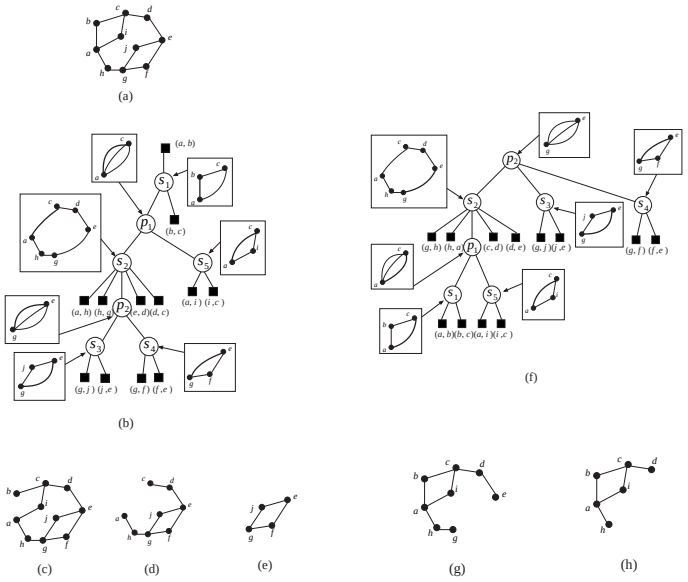


図 2.5: (a) 最大次数 3 の 2 連結グラフ G, (b) G の SPQ-tree $\mathcal{T}$, (c) S-node s_1 に関連づけられたグラフ, (d) s_2 に関連づけられたグラフ, (e) P-node p_2 に関連づけられたグラフ, (f) $\mathcal{T}$ の根を p_2 に置き換えたもの, (g) s_1 に関連づけられたグラフ, (h) その核グラフ.

基本的なアイディアとしては，直並列グラフを Battista と Tamassia らによって提案された SPQR 木 (ここではその特殊な場合の SPQ 木) に分解し，その木の葉の方から根に向かって描画を与えてゆく．すなわち，部分的な描画を組み合わせて全体の描画を構築していくことになる．図 2.5 は，SPQ 木の例を示している．各ノードは元のグラフの部分グラフ (厳密には少し異なる) に対応する直並列グラフである．

ここで，各ノードに対応する直並列グラフの描画を考える際に，始点と終点の位置によって，図 2.6 に示される 3 種類のパターンを与える．この 3 パターンのうち，L-shape drawing が可能ならばそうするが，そうでないときには side-on drawing, diagonal drawing の順で優先して描画をしていく．こうすることで，部分の描画と，それを組み合わせて得られる，より大きな部分の描画のパターンを限定することができ，最終的に全体の描画が得られれば与えられた直並列グラフが折れ曲がりなし直交描画可能かどうか判定できるということを示した．

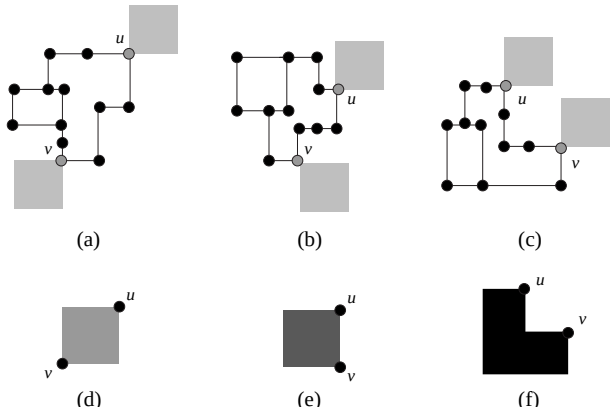


図 2.6: u と v が始点･終点になっているような直並列グラフの描画パターン: (a) diagonal drawing, (b) side-on drawing, (c) L-shape drawing, (d)-(f) それぞれの簡単化したイメージ.

5　平面グラフの矩形勢力描画

平面グラフ G の格子描画において，G の辺 e を対角線とする軸平行な長方形を e の **勢力矩形** と呼ぶ．G の各辺 (u, v) の勢力矩形領域内に (u, v) 以外の点が含まれないような G の格子描画を **矩形勢力描画 (Rectangle-of-Influence Drawing)** と呼ぶ．以下本文では矩形勢力描画のことを簡単のため RI 描画と表記する，RI 描画では，単なる格子描画よりも点と辺の距離が離れて描画されるので，同じグラフの描画でもより見やすくなる場合が多い (図 2.7(a) および 2.7(b) 参照).

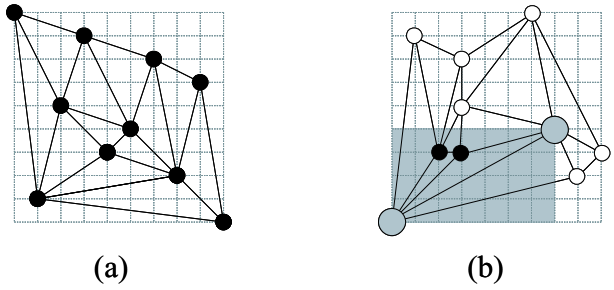


図 2.7: (a)G の RI 描画，(b)RI 描画でない G の格子描画.

勢力矩形を矩形の境界線を含む閉領域とみなしたものを **勢力閉矩形** と呼び，そのときの RI 描画を **閉 RI 描画** という．同様に，勢力矩形を

矩形の境界線を含まない開領域とみなしたものを **勢力開矩形** と呼び，そのときの RI 描画を **開 RI 描画** という．したがって，図 2.8(b) のように閉 RI 描画では各辺の勢力矩形にもその辺の端点以外の辺があってはいけない．一方，図 2.8(c) のように開 RI 描画では辺の勢力矩形の境界上にその辺の端点以外の点があってもよい．平面グラフ G が閉 RI 描画を持つための必要十分条件と，線形時間描画アルゴリズムは知られている．G が閉 RI 描画を持つための必要十分条件はむろん G が開 RI 描画を持つための十分条件である．しかし，G が開 RI 描画をもつための良い必要十分条件は知られていない．

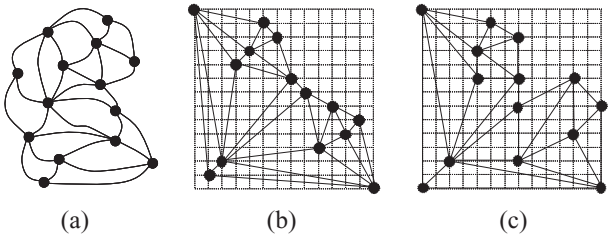


図 2.8: (a) 平面グラフ G，(b) 閉 RI 描画，(c) 開 RI 描画.

本研究では，まず，外面を含む全ての面が三角形である “三角化平面グラフ”G がある条件を満足する開 RI 描画を持つための必要十分条件を与えるとともに，G が図 2.9 のように $W + H = n$ なる整数格子内に線形時間で描画するアルゴリズムを与えた．次に全ての内面が三角形である “内部三角化平面グラフ G が開 RI 描画を持つための必要十分条件を与えるとともに，G を 図 2.10 のように $W \leq n-1$ かつ $H \leq n-1$ なる整数格子内に線形時間で描画するアルゴリズムを与えた．

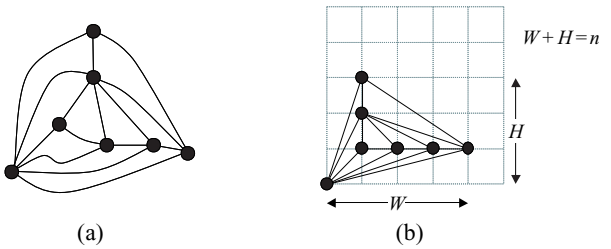


図 2.9: (a) 三角化平面グラフ G，(b)G の開 RI 描画.

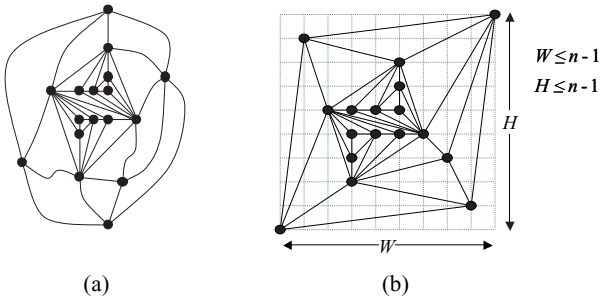


図 2.10: (a) 内部三角化平面グラフ G，(b)G の開 RI 描画.

6 Web 情報発見への応用

近年，急速に発展しているウェブ (World Wide Web) は, 情報を得る手段として日常に欠かせないものとなっている．ウェブから必要な情報を発見する手段としては, Google, Yahoo!, Goo, Infoseek などの検索エンジンが代表的なものである．これらの検索エンジンは, ユーザーの入力キーワードを含んでいるページを見つけるテキストに基づいた手法を基本として用いている．

これに対して，ウェブのハイパーリンク構造を利用した情報発見手法の研究も進められている．このリンクを用いた手法は, テキストを用いた手法のように同綴異義語やダミーキーワードなどの言語的問題に惑わされないという長所がある．リンクを情報発見に用いるための基本的な考えは, あるページ u からリンクされている ページ v は, u の作者にとって価値のある情報を含んでいる可能性が高いという仮定であり, これらの研究のほとんどは，以下のような枠組みに基づいている．(1) ウェブ中のページ群の URL とリンクのデータを収集する．(2) このデータからウェブグラフを作成する．(3) ウェブグラフ中の特徴的な部分グラフ構造を互いに関連しているページまたはサイトの集合である**コミュニティ**として抽出する．なお, 点集合 V がウェブページの集合を表し, 辺集合 E が V 中のページ間のリンクを表す有向グラフ $G = (V, E)$ を, ウェブグラフと呼ぶ．

リンク構造を用いてコミュニティを求める手法の研究としてよく知られたものに，Kleinberg の提案した HITS，Kumar らの trawling, Flake ら

による max-flow based method などがある．とくに, max-flow based method はユーザーが与えたページ群 (以下では**シードページ群**と呼ぶ) に関連するコミュニティを求めることができる手法である．

一方, 近年浅野らがリンク構造を用いてコミュニティを求める手法のための, サイトを用いた新しい枠組みを提案し, trawling などを用いてこの枠組みの有効性を示した．この枠組みは, 次のようになっている．(1) ウェブ中のページ群の URL とリンクのデータを収集する．(2) このデータから**フィルタ**手法を用いて**ディレクトリベースドサイト**を抽出する．(3) ディレクトリベースドサイトを点とし, ディレクトリベースドサイト間のリンクを辺とする**サイト間グラフ**を作成する．(4) サイト間グラフ中の特徴的な部分グラフ構造を**コミュニティ**として抽出する．

すなわち, 従来の枠組みではページを単位として用いていたのに対して, この枠組みではサイト (正確にはその近似的なモデルであるディレクトリベースドサイト) を単位として用いているといえる．これは, あるサイト A から他のサイト B へのリンクが, そのサイト A の作者にとって価値のある情報への参照を表している可能性が高いのに対して, サイト内のリンクはサイト内のページを見やすく整理するというナビゲーション目的で作られていることが多いため, リンクを用いた情報発見には両者を区別して用いることが重要と考えられるからである．

もっとも, サイトという言葉は日常的に用いられているが，それ自体曖昧な概念であり，唯一の定義もない．たとえ, いくつかの研究で用いられている「ひとりの個人，ひとつの企業，ひとつの集団がつくるページの集合をそれぞれサイトとする」という定義を用いたとしても, ウェブのページには作者の情報は一般的には含まれていないので，サイトを計算することは困難であると考えられてきた．

これに対して，近年，浅野らによって，ある時点での URL とリンクのデータ (スナップショットと呼ぶ) からこの**ディレクトリベースドサイト**というモデルと**フィルタ**という手法を用いて，サイトを近似的ではあるが実用的には十分な精度で識別する方法が発表された．さらに, これらの研究では, trawling と彼らの提案した極大クリーク法を用いて, サイトを用いた枠組みがコミュニティ発見に役立つこと, とくに個人サイトを含むコミュニティを多く見つけることに大きな効果があることを示している．だが, リンクを用いた有力なコミュニティ発見法である max-flow based method に関しては, この枠組みがどのような効果を持つかはわかっていない．

本研究では，このサイト識別の方法と豊田，喜連川らによって収集・作成された 2003 年度 2 月の .jp ドメインを主体とした日本語ページからなるスナップショットを用いて，実際にサイトのデータとサイト間グラフのデータを構築し，max-flow based method をサイト間グラフとウェブグラフ両方の上で実行し，双方の性能を評価した．また，ウェブグラフ上で max-flow based method を実行する際に精度 (コミュニティ内の実際に関連しているページの割合) を落とす原因を指摘し，サイトを用いることによって解決する方法を示した．結果として，サイト間グラフを用いた方が，コミュニティのサイズも大きくなる上に，精度も良くなることを確かめた．

さらに，サイト間グラフのリンク，サイト内のリンクを描画してコミュニティとリンクの関係をわかりやすく図示するためのツール (図 2.11 参照) を上述のグラフ描画アルゴリズムを応用して開発した．

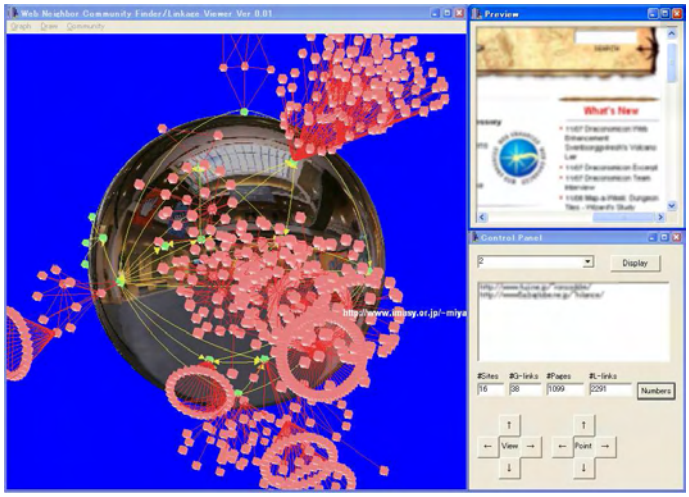


図 2.11: リンク描画ツール．

研究業績一覧

著書

1. Md. Saidur Rahman and Takao Nishizeki: "Planar Graph Drawing, Lecture Notes Series on Computing Vol. 12", World Scientific, 2004 年.

学術論文

1. X. Zhou, Y. Matsuo and T. Nishizeki: "List total colorings of series-parallel graphs", Journal of Discrete Algorithms, 3 巻 1 号, 47–60, 2005 年 3 月.
   概要: A total coloring of a graph G is a coloring of all elements of G, i.e., vertices and edges, in such a way that no two adjacent or incident elements receive the same color. Let $L(x)$ be a set of colors assigned to each element x of G. Then a list total coloring of $G$is a total coloring such that each element x receives a color contained in $L(x)$. The list total coloring problem asks whether G has a list total coloring. In this paper, we first show that the list total coloring problem is NP-complete even for series-parallel graphs. We then give a sufficient condition for a series-parallel graph to have a list total coloring, that is, we prove a theorem that any series-parallel graph G has a list total coloring if $|L(v)| \geq \min\{5, \Delta+1\}$ for each vertex v and $|L(e)| \geq \max\{5, d(v)+1, d(w)+1\}$ for each edge $e = vw$, where Δ is the maximum degree of G and $d(v)$ and $d(w)$ are the degrees of the ends v and w of e, respectively. The theorem implies that any series-parallel graph G has a total coloring with $\Delta + 1$ colors if $\Delta \geq 4$. We finally present a linear-time algorithm to find a list total coloring of a given series-parallel graph G if G satisfies the sufficient condition.

2. Md. S. Rahman, N. Egi and T. Nishizeki: "No-bend orthogonal drawings of subdivisions of planar triconnected cubic graphs", IEICE Trans. INF. SYST., E88-D No.1, 23–30, 2005 年 1 月.
   概要: A plane graph is a planar graph with a fixed embedding. In a no-bend orthogonal drawing of a plane graph, each vertex is drawn as a point and each edge is drawn as a single horizontal or vertical line segment. A planar graph is said to have a no-bend orthogonal drawing if at least one of its plane embeddings has a no-bend orthogonal drawing. In this paper we consider a class of planar graphs, called subdivisions of planar triconnected cubic graphs, and give a linear-time algorithm to examine whether such a planar graph G has a no-bend orthogonal drawing and to find one if G has.

3. Yasuhito Asano, Hiroshi Imai, Masashi Toyoda and Masaru Kitsuregawa: "Finding Neighbor Communities in the Web using an Inter-Site Graph", IEICE Trans. Inf. Syst., E87-D No. 9, 2163–2170, 2004 年 9 月.
   概要: In this paper, we present Neighbor Community Finder (NCF, for short), a tool for finding Web communities related to given URLs. While existing link-based methods of finding communities, such as HITS, trawling, and Companion, use algorithms running on a Web graph whose vertices are pages and edges are links on the Web, NCF uses an algorithm running on an *inter-site graph* whose vertices are sites and edges are *global-links* (links between sites). Since the phrase "Web site" is used ambiguously in our daily life and has no unique definition, NCF uses *directory-based sites* proposed by the authors as a model of Web sites. NCF receives URLs interested in by a user and constructs an inter-site graph containing neighbor sites of the given URLs by using a method of identifying directory-based sites from URL and link data obtained from the actual Web on demand. By

computational experiments, we show that NCF achieves higher quality than Google's "Similar Pages" service for finding pages related to given URLs corresponding to various topics selected from among the directories of Yahoo! Japan.

4. Yasuhito Asano, Tsuyoshi Ito, Hiroshi Imai, Masashi Toyoda and Masaru Kitsuregawa:
"Compact Encoding of the Web Graph Exploiting Various Power Distributions", IEICE Trans. Fundamentals, Special Section on Discrete Mathmatics and Its Applications, E87-A No. 5, 1183–1184, 2004 年 5 月.
概要: Compact encodings of the web graph are required in order to keep the graph on the main memory and to perform operations on the graph efficiently. In this paper, we propose a new compact encoding of the web graph. It is 10% more compact than Link2 used in the Connectivity Server of Altavista and 20% more compact than the encoding proposed by Guillaume et al. in 2002 and is comparable to it in terms of extraction time.

5. X. Zhou and T. Nishizeki:
"Algorithm for the cost edge-coloring of trees", Journal of Combinatorial Optimization, 8 巻 1 号, 97–108, 2004 年 3 月.
概要: Let C be a set of colors, and let be a cost function which assigns a real number $\omega(c)$ to each color C in C. An edge-coloring of a graph G is to color all the edges of G so that any two adjacent edges are colored with different colors. In this paper we give an efficient algorithm to find an optimal edge-coloring of a given tree T, that is, an edge-coloring f of T such that the sum of costs $\omega(f(e))$ of colors $f(e)$ assigned to all edges e is minimum among all edge-colorings of T. The algorithm takes time $O(n^2)$ if n is the number of vertices and is the maximum degree of T.

6. S. Isobe, X. Zhou and T. Nishizeki:
"Cost total colorings of trees", IEICE Trans. INF. SYST., E87-D No.2, 337–342, 2004 年 2 月.
概要: A total coloring of a graph G is to color all vertices and edges of G so that no two adjacent or incident elements receive the same color. Let C be a set of colors, and let ω be a cost function which assigns to each color c in C a real number $\omega(c)$ as a cost of c. A total coloring f of G is called an optimal total coloring if the sum of costs $\omega(f(x))$ of colors $f(x)$ assigned to all vertices and edges x is as small as possible. In this paper, we give an algorithm to find an optimal total coloring of any tree T in time $O(n^3)$ where n is the number of vertices in T and is the maximum degree of T.

7. T. Nishizeki, K. Miura and Md. S. Rahman:
"Algorithms for drawing plane graphs", IEICE Trans. INF. SYST., E87-D No.2, 281–289, 2004 年 2 月.
概要: Graph drawing addresses the problem of constructing geometric representation of information and finds applications in almost every branch of science and technology. Efficient algorithms are essential for automatic drawings of graphs, and hence a lot of research has been carried out in the last decade by many researchers over the world to develop efficient algorithms for drawing graphs. In this paper we survey the recent algorithmic results on various drawings of plane graphs: straight line drawing, convex drawing, orthogonal drawing, rectangular drawing and box-rectangular drawing.

8. Md. Saidur Rahman, Takao Nishizeki and Shubhashis Ghosh:
"Rectangular Drawings of Planar Graphs", Journal of Algorithms, 50 巻 1 号, 62–78, 2004 年 1 月.

概要: A plane graph is a planar graph with a fixed embedding in the plane. In a rectangular drawing of a plane graph, each vertex is drawn as a point, each edge is drawn as a horizontal or vertical line segment, and each face is drawn as a rectangle. A planar graph is said to have a rectangular drawing if at least one of its plane embeddings has a rectangular drawing. In this paper we give a linear-time algorithm to examine whether a planar graph G of maximum degree three has a rectangular drawing or not, and to find a rectangular drawing of G if it exists.

研究会等

1. 伴野幸造, 折原慎吾, 水木敬明, 西関隆夫:
"電子透かしの最良安全度について", SCIS 2005, 727–732, 2005 年.
概要:

2. Kazuyuki Miura, Hiroki Haga and Takao Nishizeki:
"Inner Rectangular Drawings of Plane Graphs", ISAAC 2004, 693–704, 2004 年.
概要: A drawing of a plane graph is called an inner rectangular drawing if every edge is drawn as a horizontal or vertical line segment so that every inner face is a rectangle. In this paper we show that a plane graph G has an inner rectangular drawing D if and only if a new bipartite graph constructed from G has a perfect matching. We also show that D can be found in time $O(n^{1.5}/\log n)$ if G has n vertices and a sketch of the outer face is prescribed, that is, all the convex outer vertices and concave ones are prescribed.

3. Md. S. Rahman, K. Miura and T. Nishizeki:
"Octagonal drawings of plane graphs with prescribed face areas", WG 2004, LNCS 3533, 320–331, 2004 年.
概要: An orthogonal drawing of a plane graph is called an octagonal drawing if each inner face is drawn as a rectilinear polygon of at most eight corners and the contour of the outer face is drawn as a rectangle. A slicing graph is obtained from a rectangle by repeatedly slicing it vertically and horizontally. A slicing graph is called a good slicing graph if either the upper subrectangle or the lower one obtained by any horizontal slice will never be vertically sliced. In this paper we show that any good slicing graph has an octagonal drawing with prescribed face areas, in which the area of each inner face is equal to a prescribed value. Such a drawing has practical applications in VLSI floorplanning. We also give a linear-time algorithm to find such a drawing. We furthermore present a sufficient condition for a plane graph to be a good slicing graph, and give a linear-time algorithm to find a tree-structure of slicing paths for a graph satisfying the condition.

4. T. Ito, X. Zhou and T. Nishizeki:
"Partitioning a weighted graph to connected subgraphs of almost uniform size", WG 2004, LNCS 3533, 365–376, 2004 年.
概要: Assume that each vertex of a graph G is assigned a nonnegative integer weight and that l and u are nonnegative integers. One wish to partition G into connected components by deleting edges from G so that the total weight of each component is at least l and at most u. Such an "almost uniform" partition is called an (l, u)-partition. We deal with three problems to find an (l, u)-partition of a given graph. The minimum partition problem is to find an (l, u)-partition with the minimum number of components. The maximum partition problem is defined similarly. The p-partition problem is to find an (l, u)-partition with a fixed number p of components. All these problems are NP-complete or NP-hard even for series-parallel graphs. In this paper we show that both the mini-

mum partition problem and the maximum partition problem can be solved in time $O(u^4n)$ and the p-partition problem can be solved in time $O(p^2u^4n)$ for any series-parallel graph of n vertices. The algorithms can be easily extended for partial k-trees, that is, graphs with bounded tree-width.

5. K. Koizumi, T. Mizuki and T. Nishizeki: "Necessary and sufficient numbers of cards for the transformation protocol", COCOON 2004, LNCS 3106, 92–101, 2004年.
概要: The transformation protocol can make two players share a secret key using a random deal of cards. A sufficient condition on the number of cards for the transformation protocol to succeed was known. However, it has been an open problem to obtain a necessary and sufficient condition. This paper improves the transformation protocol and gives a necessary and sufficient condition for the improved transformation protocol to succeed.

6. K. Miura, M. Azuma and T. Nishizeki: "Canonical decomposition, realizer, schnyder labeling and orderly spanning trees of plane graphs (extended abstract)", COCOON 2004, LNCS 3106, 92–101, 2004年.
概要: A canonical decomposition, a realizer, a Schnyder labeling and an orderly spanning tree of a plane graph play an important role in straight-line grid drawings, convex grid drawings, floor-plannings, graph encoding, etc. It is known that the triconnectivity is a sufficient condition for their existence, but no necessary and sufficient condition has been known. In this paper, we present a necessary and sufficient condition for their existence, and show that a canonical decomposition, a realizer, a Schnyder labeling, an orderly spanning tree, and an outer triangular convex grid drawing are notions equivalent with each other. We also show that they can be found in linear time whenever a plane graph satisfies the condition.

7. Md. S. Rahman, N. Egi and T. Nishizeki: "No-bend orthogonal drawings of subdivisions of planar triconnected cubic graphs", The 11th International Symposium on Graph Drawing, LNCS 2912, 387–392, 2004年.
概要: A plane graph is a planar graph with a fixed embedding. In a no-bend orthogonal drawing of a plane graph, each vertex is drawn as a point and each edge is drawn as a single horizontal or vertical line segment. A planar graph is said to have a no-bend orthogonal drawing if at least one of its plane embeddings has a no-bend orthogonal drawing. In this paper we consider a class of planar graphs, called subdividions of planar triconnected cubic graphs, and give a linear-time algorithm to examine whether such a planar graph G has a no-bend orthogonal drawing and to find one if G has.

8. Yasuhito Asano and Takao Nishizeki: "Web-linkage Viewer: Drawing Links in the Web based on a Site-oriented Framework", The 11th International Symposium on Graph Drawing, LNCS 2912, 498–499, 2004年.
概要: In recent years, link-based information retrieval methods from the Web are developed, such as HITS and Trawling. Since these methods utilize characteristic graph structures of links in the Web, analyzing the links by drawing them understandably will play an important role in the link-based information retrieval. Moreover, Asano et al. have shown that a framework using a site as a unit of information is more natural and useful for link-based information retrieval than the existing framework using a page as a unit. Therefore, we should distinguish links inside a site (called *local-links*) between links between sites (called *global-*

links) and analyze their own graph structures. However, existing drawing tools, such as Gravis and H3Viewer, do not distinguish local-links between global-links, and therefore they cannot draw graph structures of these links understandably. In this paper, we propose a new drawing tool, named *Web-linkage Viewer*, in order to draw graph structures in the Web according to the site-oriented framework.

9. 浅野泰仁, 吉田雄介, 西関隆夫, 豊田正史, 喜連川優:
"サイト間グラフの最小カットを用いたウェブ上のコミュニティ発見法", 情報処理学会研究報告 アルゴリズム研究会, 2004-AL-95, 57–64, 2004 年 5 月.
概要: 近年, ウェブのハイパーリンク構造を利用した情報発見手法の研究が進められているが, これに対してサイトを用いた新しい枠組みが提案され, trawling などを用いてこの枠組みの有効性が示されている. 一方, ユーザーによって指定されたページに関連するページの集合, すなわちコミュニティ, を求める手法として, Flake らによって最小カット法が提案されている. しかし, この手法はリンクのグラフ構造に対して最小カットを見つけて, コミュニティを求めており, サイトを用いた枠組みが最小カット法にどれだけ有用であるかはわかっていない. 本論文では, 浅野らによって提案されたサイト識別の方法と豊田, 喜連川らによって収集, 作成された 2003 年 2 月の日本語ページからなる URL とリンクのデータを用いて, 既存のページを単位とした枠組みとサイトを用いた枠組み双方で最小カット法によって様々なトピックに関してコミュニティを得る実験をすることによって, 双方の性能を評価した. 結果として, サイトを用いた枠組みを用いた最小カット法は既存の枠組みと比べて精度をほとんど落とさずに, 平均 2.5 倍程度の大きさのコミュニティを得られることがわかった.

10. Kazuyuki Miura, Hiroki Haga and Takao Nishizeki:
"Inner Rectangular Drawings of Plane Graphs", 電子情報通信学会技術研究報告 コンピュテーション研究会, COMP2004-35, 1–8, 2004 年 9 月.
概要: 平面グラフ G の各内面が長方形になるように各辺を水平線分あるいは垂直線分で描くことを, G の内部矩形描画と呼ぶ. 本論文では G が内部矩形描画 D をもつための必要十分条件は G から新しく作られた 2 部グラフが完全マッチングを持つことであることを示す. また, 点数 n の平面グラフ G とその外面の概形が与えられたとき, 即ち外面上の全ての点が凸頂点であるか凹頂点であるかが指定されているとき, D は $O(n^{1.5}/\log n)$ 時間で求めることができることを示す.

11. Yasuhito Asano, Takaaki Mizuki and Takao Nishizeki:
"On the t-safety of a key-sharing graph", 電子情報通信学会技術研究報告 コンピュテーション研究会, COMP2004-36, 9–17, 2004 年 9 月.
概要: 複数の人間 (参加者と呼ぶ) がいて, 初期秘密鍵と呼ばれる秘密鍵を共有している参加者のペアが何組かあるものとする. さらに, これらの参加者とは別の盗聴者がいるものとする. 鍵共有グラフと呼ばれる無向グラフ G は, このペアを表すものである. G の各点は参加者に対応し, 各辺は初期秘密鍵を共有するペアに対応している. 各参加者は, 公衆通信網を用いてすべての参加者にメッセージを同報できる. このメッセージは, その参加者の知っている初期秘密鍵と, これまでに同報されたメッセージから作成される. すべてのメッセージは公衆通信網を用いて同報されるので, 盗聴者とすべての参加者は同報されたすべてのメッセージを聞くことができる. 盗聴者はさらにある整数 $t \geq 0$ 個の初期秘密鍵をあらかじめ盗んでいるものとする. この条件の下で, すべての参加者がひとつの共通秘密鍵を共有したいものとする. 本論文では, すべての参加者がひとつの共通秘密鍵を安全に共有できるための必要十分条件は、鍵共有グラフ G が $(t+1)$ 個の辺素な全域木をもつことであるということを証明する.

学会大会等

1. 浅野泰仁:
   “A Site-oriented Framework for Mining Communities”, Workshop on New Horizons in Computing, 2005, 2005 年 3 月.

C02: 連続と離散の統合によるロバストアルゴリズム構築

杉原 厚吉　室田 一雄　今井 浩　松井 知己　岩田 覚　大石 泰章　西田 徹志　松浦 史郎

東京大学 大学院 情報理工学系研究科
〒 113-8656 東京都文京区本郷 7-3-1
sugihara@mist.i.u-tokyo.ac.jp

1　はじめに

本研究の目的は，今まで連続計算の分野と離散計算の分野に分かれてそれぞれ独立になされてきたアルゴリズム研究の知見を融合し，両者の手法の長所を補完し合うことによって，諸計算のロバスト性を確保するための計算原理を開拓することである．この目的に沿って，代数計算，幾何計算，確率計算，量子計算，最適化計算，制御計算において，連続と離散の知見を融合したロバストアルゴリズムを追求してきた．その主な成果をまとめる．

2　ディジタル位相優先法

私達の研究グループでは，以前から，位相構造の一貫性を数値情報より優先させることによってロバスト性を確保する幾何アルゴリズム設計法「位相優先法」を開発し，それを応用して多くのロバストソフトウェアを蓄積してきた．この設計法は，完全なロバスト性が確保でき，しかも処理速度が劣化しないという利点をもつ．しかし，設計の際に，扱う対象の位相的不変性を抽出しなければならないため，問題ごとの洞察が必要で，初心者には利用しにくいものであった．

今年度は，この位相優先法を，初心者でも使えるやさしいアルゴリズム設計法へ改良した．その基本的アイデアは次のとおりである．

位相優先法では，まず解きたい幾何問題の対象がもつ純粋に組合せ位相的性質を抽出しなければならなかった．そして，これが初心者にはむずかしかった．この難しさを回避するために，問題の解のディジタル画像近似を求め，次に，そこから位相構造を取り出し，最後にその位相構造に基づいて解を計算する．

このアイデアの有効性を確かめるために，2 次元円ボロノイ図の構成アルゴリズムを実装した．円ボロノイ図は，境界が曲線となるために，点ボロノイ図などに比べてロバスト性を確保するのが難しい．位相構造の判定をいつも正しく行うのに必要な精度は，非常に高いものになり，計算コストが大きい．したがって，位相優先法による実装が望まれていたアルゴリズムの一つである．

本実装では，まず与えられた円集合に対し，そのボロノイ図を近似的に表すディジタル画像を作る．このとき，各円が少くとも 1 個の画素を自分の領域として含む範囲で，最も低い解像度を採用する．これによって，扱う画素数を減らすことができ，計算の高速性が確保できる．実際，複数の出発点からの最短路を求めるダイクストラ法によって，円ボロノイ図のディジタル画像近似を求めることができ，画素数を N とするとその計算量は $\mathrm{O}(N \log N)$ である．

次に，このディジタル画像近似から，円ボロノイ図の領域・境界線・ボロノイ頂点の接続構造を抽出する．そして，これを真の円ボロノイ図の位相構造の近似とみなす．ディジタル画像の形式で表現されたボロノイ図は，画素による平面領域の分割構造の上に作られているため，実際に平面へ埋め込むことのできる位相構造であるという意味で，整合性が保たれている．したがって，位相優先法で位相の一貫性を保証するために利用できる．

最後に，抽出された位相構造に基づいて，ボロノイ点，ボロノイ辺を求めることによって，円ボロノイ図の近似図形を計算する．ディジタル画像近似によって位相構造の整合性は保証されているため，途中で矛盾が生じて破綻することを完全に防ぐことができる．

このアルゴリズムを円パッキング問題へ応用した例を図 2.1 に示す．図の (a) は，包含円を振ることによって中の小円が移動する途中の状態を示

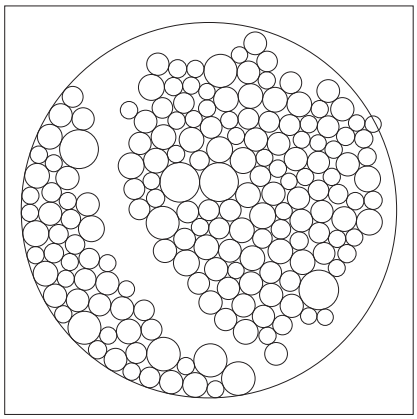


図 1(a)

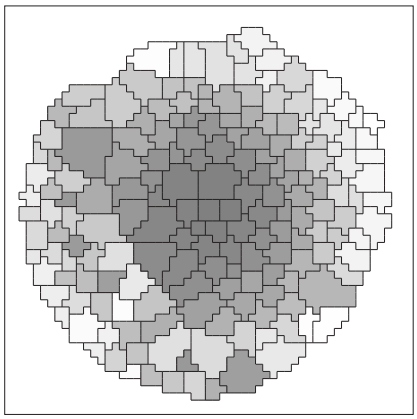


図 1(b)

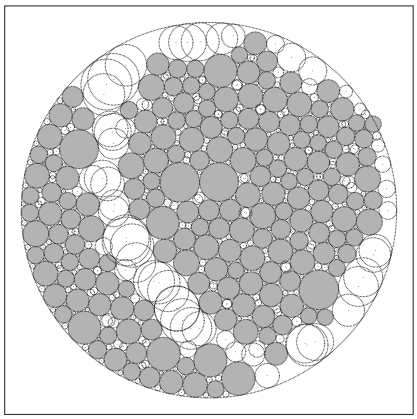


図 1(c)

図 2.1: ディジタル画像近似を利用した円ボロノイ図の計算例: (a) 円の配置, (b) 円ボロノイ図のディジタル画像近似, (c) ボロノイ点の計算結果

し, (b) はそれに対する円ボロノイ図のディジタル画像近似を示す. そして, これから抽出した位相構造に従って, ボロノイ点の中心位置とそこでの極大空円を計算した結果である. これらの情報から円パッキング問題を高速に解くことができるようになった [15].

幾何問題をディジタル画像近似を用いて解くことは, 多くの問題に対して共通の方法でほぼ機械的に実行できる. したがって, 問題ごとの個別の工夫がいらないため, 初心者にも使える技術となった.

このアイデアは, 特許申請 [16] も行った. 今後は, 球ボロノイ図など 3 次元の幾何構造の計算アルゴリズムにもこの方法を適用していく予定である.

3 離散ヘッセ行列

3.1 概要

連続変数の凸解析において, 適当な微分可能性を仮定すると, 関数 g に対して

g が凸関数
$\iff$ g のヘッセ行列が各点で半正定値
$\iff$ g の局所 2 次近似が各点で凸

が成り立つ. 本研究 [7] では, L 凸関数 [8, 9] に対して, この同値性の離散版を構築した. すなわち, 離散ヘッセ行列と局所 2 次展開を定義し, これらを用いて L 凸関数の特徴付けを行った.

一般に, 離散関数 g に関する離散ヘッセ行列 H に下記の性質を要請するのは自然であろう.

- H は g の局所的な情報により定義される対称行列
- g がアフィン関数のとき H は零行列
- H は g について線形
- $g(x) = \frac{1}{2}x^\top Ax$ のとき H は A に一致

離散関数のクラス $\mathcal{C}$ が与えられたとき, 離散ヘッセ行列を適当に定義し, さらに, 以下のような性質を持つ行列のクラス $\mathcal{H}$ を見出すことによって, 離散ヘッセ行列のクラスの特徴付けを試みる.

- 行列が $\mathcal{H}$ に属する $\iff$ その行列が, $\mathcal{C}$ に属する関数のある点における離散ヘッセ行列である.
- 関数が $\mathcal{C}$ に属する $\iff$ その関数の離散ヘッセ行列が, 各点で $\mathcal{H}$ に属する.
- 関数が $\mathcal{C}$ に属する $\iff$ その関数の離散ヘッセ行列による局所 2 次近似が, 各点で $\mathcal{C}$ に属する.

本研究で提案するL凸関数に対する離散ヘッセ行列はこれらの性質を満たしている.

3.2 結果

離散関数 $g : \mathbf{Z}^n \to \mathbf{R}$ と $p \in \mathbf{Z}^n$ に対して, 離散ヘッセ行列 $H(g;p)$ を以下で定義する:

$$\begin{aligned} H_{ij}(g;p) &= -\eta_{ij}(g;p) \quad (i \neq j), \\ H_{ii}(g;p) &= \eta_i(g;p) + \sum_{j \neq i} \eta_{ij}(g;p). \end{aligned}$$

ただし, χ_i を第 i 単位ベクトルとして,

$$\eta_{ij}(g;p) = -g(p+\chi_i+\chi_j)+g(p+\chi_i)+g(p+\chi_j)-g(p),$$
$$\eta_i(g;p) = g(p)+g(p+\mathbf{1}+\chi_i)-g(p+\mathbf{1})-g(p+\chi_i).$$

次の定理はL凸関数に対する離散ヘッセ行列のクラスを特徴付ける.

定理 次の3条件は同値である.
(a) g はL凸関数.
(b) 各 p に対して, $H_{ij}(g;p) \leq 0$ $(\forall i \neq j)$ かつ $\sum_j H_{ij}(g;p) = 0$ $(\forall i)$.
(c) 各 p に対して, $\hat{g}(q;p)$ は q に関するL凸関数.

4 量子情報幾何での連続と離散の融合

本年度の研究では, 量子通信路容量計算という誤りがある通信路をロバスト化して最大限送ることができる情報量を求める問題について, 連続と離散の融合を実現する研究を遂行することができた. 以下, この成果について簡単にまとめる.

量子通信路容量は, 量子情報理論における基本的問題であり, 量子状態を伝送する際の送信側・受信側の条件等によって様々な場合が解析されている. Holevo 容量 [5] はその中でも代表的な環境下での量子通信路の容量であり, 量子相互情報量を送信量子状態とその上の確率に関して最大化した量である. 古典通信路容量は, 古典相互情報量を送信符号上の確率に関して最大化したもので, 相互情報量がその確率に関して凹関数になっているため, 降下法によって数値的に求めることができる. Holevo 容量は, 確率について凹性が成り立つものの, 量子状態の変数については逆に凸性が成り立ち、そのために局所最適解が必ずしも大域的最適解にならず, その計算は難しいものとなる.

古典通信路容量計算の Arimoto-Blahut アルゴリズムを Holevo 容量の場合に拡張したアルゴリズムが Nagaoka [10] により提案され, Osawa, Nagaoka [11] により実装されて, Holevo 容量の加法性に関する予備的実験がなされている. しかし, 上述したことにより, 降下法であるこの方法では, 大域的最適解が得られるとは限らない. Shor [14] は, 離散個の量子状態を用いて Holevo 容量計算の部分問題を線形計画問題で表し, 無限にある量子状態から適当なものを部分最適化問題を解くことによって生成し, それを加える列生成法を用いたアルゴリズムを提案しているが, 列生成での最適化や収束性に関する性質は与えられていない.

このような状況であったところへ, 本研究では次のような展開を今年度図った. まず, Hayashi, Imai, Matsumoto, Ruskai, Shimono [4] において, 1量子ビット通信路の場合, 純粋状態に対応する Bloch 球面をメッシュ点で近似することにより, 確率変数に関する凹関数最大化を非線形計画法で解くことにより, メッシュの粗さに応じた近似解が得られることを実験的に報告した. そして, Oto, Imai, Imai, Shimono [12] において, その近似精度が Taylor 展開により最適解に十分近い近傍では説明できることを述べた. また, そこでは, 古典の場合と同様に, Holevo 容量計算が量子ダイバージェンスに関する最小包含球計算に帰着できること, および計算幾何アルゴリズムが適用できることについて触れている. これらの研究で, 近似精度を保証するためには, Bloch 球面全体を均一に近似することが必要であり, 具体的に与えられた通信路に対して通信路容量を達成するには明らかに不要な状態を考慮しないですむ仕組みは与えられていない. この点は, Shor の論文 [14] で, Holevo 容量よりも古典通信路に近い容量のアクセス情報量を計算する場合でも問題点として指摘されており, またそれが Shor が Holevo 容量計算で列生成法を提案する理由でもあった.

さらに, Hayashi, Imai, Matsumoto, Ruskai, Shimono [4] の方法が球をその球面上の均一な有限点集合の凸包で近似する内近似法であるのに対して, その球を含む凸多面体で近似する外近似法を示し, 外近似法において平面切除法を用いると

適応的に所望の近似精度で計算を行うのに必要な有限離散個の点を生成しながら近似解を求めることができることも示す．外近似のためには，球面上の点集合に対して，各点での接平面により構成される球を含む半空間の交わりとしての凸多面体を利用する．内近似に比べ，外近似は実行可能でない点，また近似精度が対応する有限点集合の内近似解よりも悪いという欠点があるが，一方で最適解の上界を与える始めての方法になっている．外近似による方法は適応的に必要部分の点の詳細化が行え，それを理論的解析が可能な簡単な量子通信路の場合で解析的に示すことを行なった．

5　スポーツスケジューリング

スポーツの試合スケジュール作成の研究は、５年程前よりアメリカを中心に大きく発展し、ソフトウェア会社の新規参入分野として注目を浴びている。アメリカで2004年春出版されたHandbook of Scheduling [1]では、組立工場の日程計画等の古典的な研究に混じって「Sports Scheduling」という独立した１章を割り当てられている程である。この背景には、大学の体育系学科の多くがスポーツマネージメント専攻を持つアメリカの、スポーツ産業の成熟がある。

これに対し、日本のプロスポーツ界で、試合スケジュール作成にソフトウェア会社等が積極的に介入した例はまだない。しかし、先の日本プロ野球リーグ制の議論を見ても分かるように、日本のプロスポーツ界はマネージメント面において大きな転換期を迎えようとしている。今後数年間の内に、日本プロスポーツにおいて収益管理やその透明性について詳細に議論されるようになることは間違いないだろう。

プロスポーツの収入の中心は、試合観戦によるものであり、その内訳は試合場に直接足を運ぶ観客と、ＴＶ等のメディアからの収入に分けられる。これに対し、魅力的な「試合スケジュール」によって収入増加を図る事は、少ない投資で堅実な収入の増加を見込める最も重要な手段の一つである。更に、試合場と試合日程を巧妙に選択してチームの移動や宿泊の費用を抑えることは、第２リーグや学生リーグにとっては重要な課題である。これに対し現状は、試合スケジュールの作成は数名の担当者の勘と経験に頼っている事が殆どである。しかし (10数チームの場合で) 数千億通りを超えるスケジュールの中から、最も良いものを選び出す作業は、勘と経験では不可能であり、前年度スケジュールを改訂する程度に留まる事が多い。

宮代隆平との共同研究 [6] により，スポーツスケジューリングにおける最適ホームアウェイテーブル作成問題対するElf予想 [2] を肯定的に解決することができた．これは，ブレーク数を最小化する問題において，最適値がチーム数未満であるかを判定する問題が多項式で解けるという予想であり，ドイツの研究グループであるElfらによって提唱されていたものである．Elfらはこの問題が特殊な最大カット問題であることから多項式時間解法が存在することを予想していたが，我々の研究によって，最大カット問題ではなく2 SAT問題として定式化することによって多項式時間で解かれる事が示された．また，最大カット問題として定式化された際の近似解法についても提案を行っている．

6　符号対称行列のSylvester指数

社会現象を線形方程式系で定式化する際には，選好順序や係数の正負などの大小関係は容易に知ることができるが，係数の数値化が困難である場合が多い．このような定性的情報のみ与えられている状況で解析を行うためには，係数行列が要素の絶対値によらず正則 (符号正則) かどうかを知る必要が生じる．この符号正則性を判定する問題の計算複雑度は長い間未解決であったが，1999年にRobertson, Seymour, Thomas [13]によって多項式時間解法が示された．本研究では, 符号正則な対称行列のSylvester符号指数を決定する多項式時間アルゴリズムを提案した．

n 次対称行列 A に対し，適当な正則行列 S による合同変換で

$$S^\top AS = \mathrm{diag}(1,\ldots,1,-1,\ldots,-1,0,\ldots,0)$$

という対角行列に変換したときの $1,-1,0$ の個数がSylvester符号指数と呼ばれる．Sylvester符号指数は, 2次形式の概形を規定する基本的な不変量である．

対称行列 A の行列式の展開項で非零なものが

存在する時，A は項別正則であると言う．正則な対称行列は項別正則である．また, 非ゼロ要素の絶対値によらず, 同じ符号要素の対称行列が全て正則であるとき, 符号正則であるという.

符号正則な対称行列に対しては，Sylvester 符号指数を行列要素の符号情報のみから一意に定まることが Hall, Li, Wang [3] によって明らかにされた．本研究では, 項別正則な対称行列の組合せ的構造を解析することによって, 符号指数を効率的に計算するアルゴリズムを設計した.

n 次正方行列 A を表現する 2 部グラフ $G(A) = (U, V; E)$ を，頂点集合 $U := \{u_1, \ldots, u_n\}$,$V := \{v_1, \ldots, v_n\}$，枝集合 $E := \{(u_i, v_j) \mid a_{ij} \neq 0, u_i \in U, v_j \in V\}$ で定める.

各頂点に高々一つの枝が接続している枝集合をマッチング, そして全ての頂点に接続している時を完全マッチングという．正方行列 A に対し，$G(A)$ が完全マッチングを持つ時，かつその時に限り A が項別正則である.

項別正則な対称行列 A に対応する 2 部グラフ $G(A) := G(U, V; E)$ の構造を調べる．項別正則性から $G(A)$ は完全マッチング M を持つ．枝集合 $X \subseteq E$ に対し，X の転置 $X^\top := \{(u_j, v_i) \mid (u_i, v_j) \in X\}$ を定義する．すると対称性より完全マッチング M の転置 $M^\top$ は完全マッチングであり，サーキット $C \subseteq E$ の転置 $C^\top$ はサーキットである．$C^\top$ と C が等しい時対称なサーキットと呼ぶ．両端点がサーキット C 上にあり C に含まれない枝を C の弦と呼ぶ．この時次の定理が成り立つ.

定理 1 項別正則な対称行列 A に対し，$G(A)$ は以下のいずれかの条件を満たす.

- $a_{ii} \neq 0$ となる (u_i, v_i) を含む完全マッチングが存在する.
- $a_{ij} = a_{ji} \neq 0$ $(i \neq j)$ となる (u_i, v_j), (u_j, v_i) を含む完全マッチングが存在する.
- $G(A)$ は弦の無い対称なサーキットの直和.

この定理を用いて, 符号正則な n 次対称行列の符号指数を, 行列要素の符号情報のみから計算するアルゴリズムを設計した．その計算量は, 非零要素数を m とするとき, $O(nm)$ である.

一方で, 項別正則とは限らない一般の対称行列に関しては, 行列要素の符号情報のみから符号指数が決定不可能かどうかを判定する問題は，NP 完全であることも明らかとなった.

7 ロバスト制御器の確率的設計

7.1 目的

非線形なパラメータ的不確かさが存在する場合のロバスト制御系設計は，古典的ではあるが依然として難しい問題である．本研究ではできるだけ保守的でない制御系設計をするために，パラメータ依存 Lyapunov 関数を使って定式化し，確率的算法を適用することを考える.

7.2 定式化

パラメータ依存 Lyapunov 関数を使う場合，ロバスト制御系の設計問題は次のように表現できる．ただし，$V(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{\theta})$ は $\boldsymbol{x} \in \mathbb{R}^n$, $\boldsymbol{y} \in \mathbb{R}^m$, $\boldsymbol{\theta} \in \Theta \subseteq \mathbb{R}^p$ の対称行列値の関数であり，$\boldsymbol{x}$ と $\boldsymbol{y}$ に関してアフィンであって，$\boldsymbol{\theta} \in \Theta$ の対称行列値の関数 $V_0(\boldsymbol{\theta}), V_1(\boldsymbol{\theta}), \ldots, V_{n+m}(\boldsymbol{\theta})$ を使って

$$V(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{\theta}) = V_0(\boldsymbol{\theta}) + \sum_{i=1}^{n} x_i V_i(\boldsymbol{\theta}) + \sum_{i=1}^{m} y_i V_{n+i}(\boldsymbol{\theta})$$

と表されるとする.

問題． 任意の $\boldsymbol{\theta} \in \Theta$ に対して

$$V(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{\theta}) \prec O$$

を満たす $\boldsymbol{y} \in \mathbb{R}^m$ が存在するような $\boldsymbol{x} \in \mathbb{R}^n$ を求めよ．ただし，$\boldsymbol{y}$ は $\boldsymbol{\theta}$ に依存してもよい． ∎

ここでパラメータ $\boldsymbol{\theta}$ に依存しない変数 $\boldsymbol{x}$ は求める制御器に対応し,

パラメータに依存する変数 $\boldsymbol{y}$ は Lyapunov 関数に対応する.

以上の問題は，関数 V が変数 $\boldsymbol{y}$ に依存しないという特別な場合には，既にこれを解くための確率的算法が構成されている．本研究ではこれを拡張し，V が $\boldsymbol{y}$ に依存する場合にも使えるような確率的算法の構成を行なう.

7.3 結果

パラメータ $\boldsymbol{\theta}$ に依存する変数 $\boldsymbol{y}$ が存在する場合に使える確率的算法を構成した．

まず，変数 $\boldsymbol{x}$ とパラメータ $\boldsymbol{\theta}$ を固定するとき，$V(\boldsymbol{x},\boldsymbol{y},\boldsymbol{\theta}) \prec O$ を満たす $\boldsymbol{y} \in \mathbb{R}^m$ が存在するということは，

$$\min_{\boldsymbol{y}\in\mathbb{R}^m} \overline{\lambda}[V(\boldsymbol{x},\boldsymbol{y},\boldsymbol{\theta})] < 0 \qquad (2.12)$$

と同値であることに注意する．ただし $\overline{\lambda}(A)$ は対称行列 A の最大の（最も正の）固有値を表すものとする．式 (2.12) の左辺 $\min_{\boldsymbol{y}\in\mathbb{R}^m} \overline{\lambda}[V(\boldsymbol{x},\boldsymbol{y},\boldsymbol{\theta})]$ は $\boldsymbol{x}$ に関して凸であるので，あとはこの関数の劣勾配さえ計算できれば，前年度構成した確率的算法が使えることになる．ところが，この関数の値は半正定値計画問題

$$\begin{aligned} &\text{minimize} \quad \lambda \quad \text{in} \quad (\lambda, \boldsymbol{y}) \\ &\text{subject to} \quad V(\boldsymbol{x},\boldsymbol{y},\boldsymbol{\theta}) - \lambda I \preceq O \end{aligned}$$

の最適値であることに注意すると，その双対問題

$$\begin{aligned} &\text{maximize} \quad \mathrm{tr}\,[UV(\boldsymbol{x},\boldsymbol{0},\boldsymbol{\theta})] \quad \text{in} \quad U \\ &\text{subject to} \quad U \succeq O, \quad \mathrm{tr}\,U = 1, \\ &\qquad\qquad \mathrm{tr}\,[UV_{n+i}(\boldsymbol{\theta})] = 0 \quad \text{for } i = 1,2,\ldots,m \end{aligned}$$

の最適解 U を使って求める劣勾配が計算できることがわかる．

以上の考察に基づき，前節の問題に対する確率的算法を構成した．構成した算法は，問題のサイズの多項式で表される数の繰り返しの後に停止し，

ほとんどの $\boldsymbol{\theta} \in \Theta$ に対して

$$V(\boldsymbol{x},\boldsymbol{y},\boldsymbol{\theta}) \prec O$$

を満たす $\boldsymbol{y} \in \mathbb{R}^m$ が存在するような $\boldsymbol{x}$ を高い信頼度で求めるか，またはそのような $\boldsymbol{x}$ が近似的な意味で存在しないことを検出する．

8 ボート航行距離方程式のロバスト解法

流れを伴う 2 次元水面上に 2 点，始点と終点が与えられとき，ボートが始点から終点まで動くのにかかる最短時間をボート航行距離と呼び，この距離を求める問題を時間項を含まない偏微分方程式の境界値問題に帰着した．この方程式をボート航行距離方程式と名付けた．この方程式は幾何光学などで知られる eikonal 方程式の拡張になっている．eikonal 方程式は Fast Marching 法という数値解法によって，効率的かつ安定に解くことができるので，その手法をボート航行距離方程式に適用したが，うまく機能しなかった．そこで，我々の方程式を効率的かつ安定に解くことができるように改良した拡張 Fast Marching 法を考案した．

本年度は，ボート航行距離方程式の次元の一般化，具体的には，流れを伴う曲面上における最短距離を求めるための偏微分方程式の構築を行った．ボート航行距離は，その作り方から 2 次元から 3 次元への拡張は容易であるので，方程式を 3 次元にし，領域を曲面に制限することで解くことができる．しかし，本研究では，曲面を平面に射影することにより，新たな方程式の構築を行った．なぜなら，次元を減らせることや，拡張 Fast Marching 法を利用することができるからである．

$\Omega \in \mathbf{R^2}$ を xy 平面上の領域，$z = h(x,y)$, $(x,y) \in \Omega$ を曲面の高さとする．曲面は微分可能とし，その偏微分を

$$\left(\frac{\partial h}{\partial x}, \frac{\partial h}{\partial y}\right) \equiv (h_x, h_y)$$

とする．さらに，曲面上には，曲面に沿う流れ $f(x,y,z) \in \mathbf{R^3}$ が与えられているとする．

流れがなければ速さ $F(x,y,z)$ で航行できるボートがこの曲面上を移動するとする．ただし，各点で $F > |f|$ を仮定する．p, q を Ω 上の点とし，曲面上の対応する点をそれぞれ $(p,h(p))$, $(q,h(p))$ とする．このとき，$(p,h(p))$ から $(q,h(q))$ へ移動するのに必要な最短時間を「曲面上のボート航行距離」と呼ぶ．

曲面上のボート航行距離を解析的に求めることは難しいので，近似計算に頼らざるを得ない．そこで，偏微分方程式を利用をするのだが，ここでは平面に射影して解く．つまり，ボートは曲面上を移動するのだが，それを射影した平面上で書き表すことを考える．

時刻 0 に $p_0 \in \Omega$ にいるとし，このボートの点 $p = (x,y)$ までの到達時間を $T(x,y)$ とする．ボートが最短時間を達成する経路に沿って進み，時刻 t で (x,y) を通過し，時刻 $t+\Delta t$ では，$(x+\Delta x, y+$

$\Delta y)$ を通過するとすると，

$$\Delta t = T(x+\Delta x, y+\Delta y) - T(x,y)$$

と表わすことができる．そして，右辺第 2 項をテイラー展開すると

$$\Delta t = T_x \Delta x + T_y \Delta y + \mathrm{O}((\Delta x)^2 + (\Delta y)^2) \quad (2.13)$$

となる．ただし，T_x, T_y は，それぞれ T の x, y 方向への偏微分を表わす．

次に，曲面上の動きを射影したときの Ω 上での動きを考える．N を曲面の法線ベクトル，S を曲面上の点 $(p_0, h(p_0))$ からの等時間曲線 Γ に対する接ベクトルとする．このとき，最短時間を達成するためには，ボートは Γ に対して入射角が垂直になるように進むのがよい．よって，時刻 t から時刻 $t+\Delta t$ の間のボートの変位は，$F(N\times S) + f\Delta t$ と書ける．ただし，法線ベクトルは $N = (-h_x, -h_y, 1)/\sqrt{1+{h_x}^2+{h_y}^2}$，接ベクトルは

$$S = \frac{(T_y, -T_x, h_y T_x - h_x T_y)}{\sqrt{T_x^2 + T_y^2 + (h_y T_x - h_x T_y)^2}}$$

である．

$f = (f_x, f_y, f_z)$ と置くと，$F(N\times S) + f\Delta t$ を Ω 上へ射影したときの x 成分，y 成分は，それぞれ

$$\Delta x = \left\{ F\frac{(1+h_y^2)T_x - h_x h_y T_y}{k} + f_x \right\} \Delta t \quad (2.14)$$

$$\Delta y = \left\{ F\frac{(1+h_x^2)T_y - h_x h_y T_x}{k} + f_y \right\} \Delta t \quad (2.15)$$

となる．ただし，

$$k = \sqrt{(1+h_x^2+h_y^2)(T_x^2+T_y^2+(h_y T_x - h_x T_y)^2)}.$$

である．

式 (2.13)，(2.14)，(2.15) により，

$$F\sqrt{\frac{(1+h_y^2)T_x^2 - 2h_x h_y T_x T_y + (1+h_x^2)T_y^2}{1+h_x^2+h_y^2}} = 1 - T_x f_x - T_y f_y \quad (2.16)$$

を得る．

式 (2.16) を $T(p_0) = 0$ の境界条件をもとで解くことによって，曲面上のボート航行距離を求めることができる．

これにより，航路や飛行路の最短経路問題に応用が期待される．タンカーや船が海を航行すれとする．そのとき，海の表面は海流を伴う曲面である．また，長距離を飛ぶ飛行機は，気流に影響されながら，ほとんどの時間をある決められた高度を保ちつつ移動する．ゆえに，これも流れを伴う曲面となる．

今後は，$F > |f|$ と仮定していた条件を取り除いても効率的かつ安定に解くことのできる手法の開発を行っていきたい．

参考文献

[1] K. Easton, G. Nemhauser and M. Trick, “Sports Scheduling”, In: Handbook of Scheduling: Algorithms, Models, and Performance Analysis, J. Y-T. Leung and J. H. Anderson (Eds.), Chapman & Hall, 2004.

[2] M. Elf, M. Jünger and G. Rinaldi, “Minimizing breaks by maximizing cuts,” Operations Research Letters, Vol. 31 (2003), pp. 343–349.

[3] F. J. Hall, Z. Li, and D. Wang, “Symmetric sign pattern matrices that require uniquie inertia”, Linear Algebra Appl., 338 (2001), pp.153–169.

[4] M. Hayashi, H. Imai, K. Matsumoto, M. B. Ruskai and T. Shimono, “Qubit Channels Which Require Four Inputs to Achieve Capacity”, Quantum Information and Computation, to appear.

[5] A. S. Holevo, “The Capacity of the Quantum Channel with General Signal States”, IEEE Trans. Inf. Theory, Vol. 44, No. 1 (1998), pp. 269–273.

[6] R. Miyashiro and T. Matsui, “A Polynomial Time Algorithm to Find an Equitable Home-away Assignment”, Operations Research Letters, Vol. 33 (2004), pp. 235–241.

[7] S. Moriguchi and K. Murota: Discrete Hessian Matrix for L-convex Functions, *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, to appear.

[8] 室田一雄: 離散凸解析, 共立出版, 2001.

[9] K. Murota: *Discrete Convex Analysis*, SIAM, 2003.

[10] H. Nagaoka, "Algorithms of Arimoto-Blahut Type for Computing Quantum Channel Capacity", Proc. 1998 IEEE International Symposium on Information Theory, (1998), p. 354.

[11] S. Osawa and H. Nagaoka, "Numerical Experiments on the Capacity of Quantum Channel with Entangled Input States", IEICE Trans. Fundamentals, Vol. E84-A, No. 10 (October 2001), pp. 2583–2590.

[12] M. Oto, H. Imai, K. Imai and T. Shimono, "Computational Geometry of Bloch Sphere", Proc. ERATO Conference on Quantum Information Science (EQIS 2004), 2004, pp. 156–157.

[13] N. Robertson, P. D. Seymour, and R. Thomas, "Permanents, Pfaffian orientations, and even directed circuits", Ann. Math., (2) 150, no. 3 (1999), pp. 929–975.

[14] P. W. Shor, "Capacities of Quantum Channels and How to Find Them", Mathematical Programming, Vol. 97 (2003), pp. 311–335.

[15] K. Sugihara, "Robust Geometric Computation Based on Digital Topology", Proceeding of the 10th Conference on Computing and Combinatorics, COCOON2004, Teju, Korea, Augurst 17–20, 2004, pp. 3–12.

[16] 杉原厚吉，松浦史郎, "勢力圏図計算装置及びプログラム", 特許出願, 特願 2004-230652, 2004 年 8 月 6 日.

研究業績一覧

学術論文

1. Yasuhito Asano, Tuyoshi Ito, Hiroshi Imai, Masashi Toyoda, Masaru Kitsuregawa: "Compact Encoding of the Web Graph Exploiting Various Power Distributions", IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E87-A, No. 5, 1183-1184, 2004 年.
   概要: Compact encodings of the web graph are required in order to keep the graph on the main memory and to perform operations on the graph efficiently. In this paper, we propose a new compact encoding of the web graph. It is 10% more compact than Link2 used in the Connectivity Server of Altavista and 20% more compact than the encoding proposed by Guillaume *et al.* in 2002 and is comparable to it in terms of extraction time.

2. Yasuhito Asano, Hiroshi Imai, Masashi Toyoda, Masaru Kitsuregawa: "Finding Neighbor Communities in the Web Using an Inter-site Graph", IEICE Transaction on Information and Systems, Vol. E87-D, No. 9, 2163-2170, 2004 年.
   概要: In this paper, we present Neighbor Community Finder (NCF, for short), a tool for finding Web communities related to given URLs. While existing link-based methods of finding communities, such as HITS, trawling, and Companion, use algorithms running on a Web graph whose vertices are pages and edges are links on the Web, NCF uses an algorithm running on an inter-site graph whose vertices are sites and edges are global-links (links between sites). Since the phrase "Web site" is used ambiguously in our daily life and has no unique definition, NCF uses directory-based sites proposed by the authors as a model

of Web sites. NCF receives URLs interested in by a user and constructs an inter-site graph containing neighbor sites of the given URLs by using a method of identifying directory-based sites from URL and link data obtained from the actual Web on demand. By computational experiments, we show that NCF achieves higher quality than Google's "Similar Pages" service for finding pages related to given URLs corresponding to various topics selected from among the directories of Yahoo! Japan.

3. Masahito Hayashi, Hiroshi Imai, Keiji Matsumoto, Mary Beth Ruskai, Toshiyuki Shimono:
"Qubit Channels which Require Four Inputs to Achieve Capacity: Implications for Additivity Conjectures", Quantum Information and Computation, Vol. 5, No. 1, 13-31, 2005 年.
概要: An example is given of a qubit quantum channel which requires four inputs to maximize the Holevo capacity. The example is one of a family of channels which are related to 3-state channels. The capacity of the product channel is studied and numerical evidence presented which strongly suggests additivity. The numerical evidence also supports a conjecture about the concavity of output entropy as a function of entanglement parameters. However, an example is presented which shows that for some channels this conjecture does not hold for all input states. A numerical algorithm for finding the capacity and optimal inputs is presented and its relation to a relative entropy optimization discussed.

4. Hiroshi Hirai, Kazuo Murota:
"M-convex Functions and Tree Metrics", Japan Journal of Industrial and Applied Mathematics, Vol. 21, No. 3, pp. 391-403, 2004 年.
概要: We reveal a close relationship between quadratic M-convex functions and tree metrics: A quadratic function defined on the integer lattice points is M-convex if and only if it has a tree representation. Furthermore, a discrete analogue of the Hessian matrix is defined for functions on the integer points. A function is M-convex if and only if the negative of the 'discrete Hessian matrix' is a tree metric matrix at each integer point. Thus, the M-convexity of a function can be characterized by that of its local quadratic approximations.

5. Satoru Iwata, Satoko Moriguch, Kazuo Murota:
"A Capacity Scaling Algorithm for M-convex Submodular Flow", Mathematical Programming, 2004 年.
概要: This paper presents a faster algorithm for the M-convex submodular flow problem, which is a generalization of the minimum-cost flow problem with an M-convex cost function for the flow-boundary, where an M-convex function is a nonlinear nonseparable discrete convex function on integer points. The algorithm extends the capacity scaling approach for the submodular flow problem by Fleischer, Iwata and McCormick (2002) with the aid of a novel technique of changing the potential by solving maximum submodular flow problems.

6. Satoru Iwata, Nozomu Zuiki:
"A Network Flow Approach to Cost Allocation in Rooted Trees", Networks, Vo. 44, No. 4, pp. 297–301, 2004 年.
概要: In the game theory approach to cost allocation, the main computational issue is an algorithm for finding solutions such as the Shapley value and the nucleolus. In this paper, we consider the problem of allocating the maintenance cost of a tree network that connects the supply source at the root to the users at the leaves. We show that the core of the game can be expressed in

terms of network flows. Based on this observation, we present $O(n \log n)$ algorithms for computing the nucleolus and the egalitarian allocation.

7. Shuji Kijima, Tomomi Matsui:
"Approximate Counting Scheme for mxn Contingency Tables", IEICE Transactions on Information and Systems, Vol. E87-D, No. 2, pp. 308–314, 2004 年.
概要: In this paper, we propose a new counting scheme for $m \times n$ contingency tables. Our scheme is a modification of Dyer and Greenhill's scheme for two rowed contingency tables. We can estimate not only the sizes of error, but also the sizes of the bias of the number of tables obtained by our scheme, on the assumption that we have an approximate sampler.

8. Tomomi Matsui, Yasuko Matsui, Yoko Ono:
"Random Generation of $2 \times 2 \times \cdots \times 2 \times J$ Contingency Tables", Theoretical Computer Science, Vol. 326, pp. 117–135, 2004 年.
概要: We propose two Markov chains for sampling $(m+1)$-dimensional contingency tables indexed by $\{1,2\}^m \times \{1,2,\ldots,n\}$. Stationary distributions of our chains are the uniform distribution and a conditional multinomial distribution (which is equivalent to the hypergeometric distribution if $m = 1$). Mixing times of our chains are bounded by $(1/2)n(n-1)\ln(N/(2^m\varepsilon)) = (1/2)n(n-1)\ln(dn/\varepsilon)$, where d is the average of the values in the cells and ε is a given error bound. We use the path coupling method for estimating the mixing times of our chains and showed that our chains mix rapidly.

9. Yuichiro Miyamoto, Tomomi Matsui:
"Linear Time Approximation Algorithm for Multicoloring Lattice Graphs with Diagonals", Journal of Operations Research Society of Japan, Vol. 47, No. 2, pp. 123–128, 2004 年.
概要: Let P be a subset of 2-dimensional integer lattice points $P = \{1,2,\ldots,m\} \times \{1,2,\ldots,n\} \subseteq \mathrm{Z}^2$. We consider the graph G_P with vertex set P satisfying that two vertices in P are adjacent if and only if Euclidean distance between the pair is less than or equal to $\sqrt{2}$. Given a non-negative vertex weight vector $\boldsymbol{w} \in \mathrm{Z}_+^P$, a multicoloring of $(G_P, \boldsymbol{w})$ is an assignment of colors to P such that each vertex $v \in P$ admits $w(v)$ colors and every adjacent pair of two vertices does not share a common color. We show the NP-completeness of the problem to determine the existence of a multicoloring of $(G_P, \boldsymbol{w})$ with strictly less than $(4/3)\omega$ colors where ω denotes the weight of a maximum weight clique. We also propose an $\mathrm{O}(mn)$ time approximation algorithm for multicoloring $(G_P, \boldsymbol{w})$. Our algorithm finds a multicoloring with at most $(4/3)\omega + 4$ colors Our algorithm based on the property that when $n = 3$, we can find a multicoloring of $(G_P, \boldsymbol{w})$ with ω colors easily, since an undirected graph associated with $(G_P, \boldsymbol{w})$ becomes a perfect graph.

10. Ryuhei Miyashiro, Tomomi Matsui:
"A Polynomial Time Algorithm to Find an Equitable Home-away Assignment", Operations Research Letters, Vol. 33, No. 3, pp. 235–241, 2004 年.
概要: We propose a polynomial time algorithm to find an equitable home-away assignment for a given timetable of a round-robin tournament. Our results give an answer to a problem raised by Elf, Jünger and Rinaldi which concerns the computational complexity of the break minimization problem in sports timetabling.

11. Satoko Moriguchi, Kazuo Murota:
"Discrete Hessian Matrix for L-convex Functions", IEICE Transactions on Fundamentals of Electronics, Communications

and Computer Sciences, 2004年.
概要: L-convex functions are nonlinear discrete functions on integer points that are computationally tractable in optimization. In this paper, a discrete Hessian matrix and a local quadratic expansion are defined for L-convex functions. We characterize L-convex functions in terms of the discrete Hessian matrix and the local quadratic expansion.

12. Kazuo Murota:
"Note on Multimodularity and L-convexity", Mathematics of Operations Research, (掲載予定).
概要: Multimodular functions and L-convex functions have been investigated almost independently, but they are, in fact, equivalent objects that can be related through a unimodular coordinate transformation. Some facts known for L-convex functions can be translated to new results for multimodular functions, and vice versa. In particular, the local optimality condition for global optimality found in the literature of multimodular functions should be rectified, and a discrete separation theorem holds for multimodular functions

13. Kazuo Murota, Akiyoshi Shioura:
"Conjugacy Relationship between M-convex and L-convex Functions in Continuous Variables", Mathematical Programming, Vol. 101, No. 3, pp. 415–433, 2004年.
概要: By extracting combinatorial structures in well-solved nonlinear combinatorial optimization problems, Murota (1996,1998) introduced the concepts of M-convexity and L-convexity to functions defined over the integer lattice. Recently, Murota–Shioura (2000, 2001) extended these concepts to polyhedral convex functions and quadratic functions in continuous variables. In this paper, we consider a further extension to more general convex functions defined over the real space, and provide a proof for the conjugacy relationship between general M-convex and L-convex functions.

14. Kazuo Murota, Akihisa Tamura:
"Proximity Theorems of Discrete Convex Functions", Mathematical Programming, Vol. A99, No. 3, pp. 539–562, 2004年.
概要: A proximity theorem is a statement that, given an optimization problem and its relaxation, an optimal solution to the original problem exists in a certain neighborhood of a solution to the relaxation. Proximity theorems have been used successfully, for example, in designing efficient algorithms for discrete resource allocation problems. After reviewing the recent results for L-convex and M-convex functions, this paper establishes proximity theorems for larger classes of discrete convex functions, L^2-convex functions and M^2-convex functions, that are relevant to the polymatroid intersection problem and the submodular flow problem.

15. Kazuo Murota, Hiroo Saito, Robert Weismantel:
"Optimality Criteria for a Class of Nonlinear Integer Programs", Operations Research Letters, Vol. 32, No. 5, pp. 468–472, 2004年.
概要: Graver's optimality conditions based on Hilbert bases apply to an integer program with linear equations and a linear objective function. We generalize this result to include a fairly large class of nonlinear objective functions. Our extension provides in particular a link between the superadditivity of the difference-objective function and the Hilbert bases of conic subpartitions of n-dimensional space.

16. Kazuo Murota, Akiyoshi Shioura:
"Fundamental Properties of M-convex and

L-convex Functions in Continuous Variables", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E87-A, No. 5, pp. 1042–1052, 2004年.

概要: The concepts of M-convexity and L-convexity, introduced by Murota (1996,1998) for functions on the integer lattice, extract combinatorial structures in well-solved nonlinear combinatorial optimization problems. These concepts are extended to polyhedral convex functions and quadratic functions on the real space by Murota–Shioura (2000, 2001). In this paper, we consider a further extension to general convex functions. The main aim of this paper is to provide rigorous proofs for fundamental properties of general M-convex and L-convex functions.

17. Kazuo Murota, Akiyoshi Shioura:
"Quadratic M-convex and L-convex Functions", Advances in Applied Mathematics, Vol. 33, No. 2, pp. 318–341, 2004年.

概要: The concepts of L-convexity and M-convexity are introduced by Murota (1996) for functions defined over the integer lattice, and recently extended to polyhedral convex functions by Murota–Shioura (2000). L-convex and M-convex functions are deeply connected with well-solvability in combinatorial optimization problems with convex objective functions. In this paper, we consider these concepts for quadratic functions and the structure of the coefficient matrices of such quadratic functions. It is shown that quadratic L-convex and M-convex functions can be characterized by nice combinatorial properties of their coefficient matrices. The conjugacy relationship between quadratic L-convex and M-convex functions is also discussed.

18. Kokichi Sugihara:
"Hyperpolygons Generated by the Invertible Minkowski Sum of Polygons", Pattern Recognition Letters, Vol. 25, pp. 551–560, 2004年.

概要: The paper gives a new formulation of the Minkowski sum of polygons. In the conventional Minkowski sum, the inverse operation is not well defined unless the polygons are restricted to be convex. In the proposed formulation, on the other hand, the set of polygons is extended to the set of "hyperpolygons" and the Minkowski sum forms a commutative group. Consequently, every polygon has its unique inverse, and the sum and the inverse operations can be taken freely. An example of a physical interpretation of the hyperpolygon is also given.

19. Kokichi Sugihara:
"Mathematics of Pictures of Impossible Objects: Human Vision vs. Robot Vision", SUGAKU EXPOSITIONS, Vol. 17, No. 125, pp. 37–49, 2004年.

概要: This paper presents a mathematical method for interpreting line drawings as polyhedral objects, and compares it with human visual perception. One of the greatest differences between machine perception and human perception is that the machine perception recognizes inconsistency strictly while the human perception sometimes reject correct pictures according to predusice. Because of this difference, there are some pictures which are called "impossible objects" although the objects are actually reconstructible from the picture.

20. Kokichi Sugihara, Masayoshi Sawai, Hiroaki Sano, Deok-Soo Kim, Donguk Kim:
"Disk Packing for the Estimation of the Size of a Wire Bundle", Japan Journal of Industrial and Applied Mathematics, Vol. 21, No. 3, pp. 259–278, 2004年.

概要: A heuristic method for packing disks in a circle is constructed, and is applied to the estimation of the sizes of holes through

which given sets of electric wires are to pass. Modern intelligent machines such as planes and cars have a variety of electric systems, and consequently a lot of electric wires run in a complicated way. These wires should pass through holes opened in the walls of the body of a machine. Those wholes should be as small as possible because larger holes weaken the body. The problem of finding the smallest hole is reduced to the problem of finding the smallest circle containing all of given disks without overlap. In the proposed method, a sufficiently large circle is initially constructed, and it is shrunk step by step while keeping all the disks inside. For this purpose a Voronoi diagram for circles is used. Computational experiments show the validity and the efficiency of the method.

21. Kenichiro Tanaka, Masaaki Sugihara, Kazuo Murota:
"Numerical Indefinite Integration by Double Exponential Sinc Method", Mathematics of Computation, Vol. 74, No. 250, pp. 655–679, 2005 年.
概要: We present a numerical method for approximating an indefinite integral by the double exponential sinc method. The approximation error of the proposed method with N integrand function evaluations is of the order of $\exp(-c_1 N/\log(c_2 N)))$ for a reasonably wide class of integrands, including those with end-point singularities. The proposed method compares favorably with the existing formulas based on the ordinary sinc method. Computational results show the accordance of the actual convergence rates with the theoretical estimate.

22. 藤村光，杉原厚吉:
"優勢領域に基づいたスポーツチームワークの定量的評価"，電子情報通信学会論文誌, Vol. J87-D-II, No. 3, pp. 818–828, 2004 年.
概要: 本研究では，選手が特定のフィールド上を自由に動き回り，目標に対して競い合うチームスポーツを対象にして，チームワークの定量的評価を行う．この種のスポーツでは，各選手が支配するフィールドを把握することがチームワーク評価への道となる．そのため，フィールドを支配関係によって分割する優勢領域図の概念を応用し，それによるチームワークの定量的評価手法を提案する．また本研究においてはこの優勢領域図の作成にあたって，実験に基づいたより現実的な運動モデルを採用している．

23. 神田毅, 杉原厚吉, 森本康彦:
"幾何アルゴリズム加速のための混合演算に関する研究"，日本応用数理学会論文誌, Vol. 14, No. 2, pp. 117–150, 2004 年.
概要: A widely used strategy to decrease the execution time of robust geometric algorithms using multiprecision integer arithmetic is the hybrid use of integer and floating-point arithmetic. In this strategy, multiprecision integer arithmetic is avoided if the sign decision in floating-point arithmetic used in advance is regarded as sufficiently reliable. It is important for this strategy to estimate the upper bound of the error calculated in floating-point arithmetic. However, the method of the estimation is not unique. The more tightly the error is estimated, the more frequently multiprecision integer arithmetic is avoided. However, a tight upper bound requires high computational cost. This paper investigates how the suitable estimation varies as the type and the scale of inputs vary. Experimental consideration is done using the incremental method for constructing the Voronoi diagram as an example of the geometric algorithm.

24. 室谷浩平, 杉原厚吉:
"大域的滑らかさを優先した標高データからの地形復元法の提案"，GIS-理論と応用, Vol. 12, No. 1, pp. 1–13, 2004 年.
概要: The purpose of this research is to

construct a surface (1) passing through all unorganized data points, (2) with G1-continuity and (3) with the minimum square-sum of the principal curvatures ${\kappa_1}^2+{\kappa_2}^2$ over the surface. In order to construct surfaces with these three characteristics, we construct the triangular mesh spanning the data points, cover it with Bezier patches, achieve continuity between patches, and minimize the curvature to prevent the surfaces from having flat places and unnecessary undulations. The performance of the proposed method is evaluated by computational experiments using actual land height data.

25. 力徳正輝，平井広志，室田一雄:
“2 段階アルゴリズムによる SVM の解法”, 日本応用数理学会論文誌, Vol. 14, No. 4, pp. 221–234, 2004 年.
概要: A two-stage algorithm is proposed for the learning phase of support vector machines (SVM). The algorithm is a combination of the Sequential Minimal Optimization (SMO) and the projected quasi Newton method. Use of the quasi Newton method in the neighborhood of optimal solutions results in a substantial improvement upon SMO in the number of iterations, and hence in numerical accuracy of the solution. Computational results on the UCI Adult and Web data set show that the two-stage algorithm performs comparably with SMO in usual parameter settings, but outperforms SMO for large C values and small tolerances.

26. 高松吉郎，原辰次，室田一雄:
“連続/離散ハイブリッド凸最適化とその最適性規準”，システム制御情報学会論文誌, Vol. 17, No. 9, pp. 409–411, 2004 年.
概要: 近年，ハイブリッドシステムのモデル予測制御などにおいて，混合整数 2 次計画問題を短時間で解くアルゴリズムの構築が求められている．一方で，最適化の分野では離散凸解析という枠組みが確立しつつある．本論文では，まず解きやすいクラスとしてハイブリッド凸関数の概念を提案する．具体的には，L ♯凸関数の概念をもとにハイブリッド L ♯凸関数を定義し，これに基づいて混合整数計画問題のサブクラスにあたるハイブリッド凸計画問題を定式化する．最後にハイブリッド L ♯凸関数に対する最適性規準を導出する．

27. Akira Fujimura, Kokichi Sugihara:
“Geometric Analysis and Quantitative Evaluation of Sport Teamwork”, International Symposium on Voronoi Diagrams in Science and Engineering, pp. 37–48, 2004 年 9 月.
概要: A quantitative method for evaluating sport teamwork is proposed. The sports considered here are team sports in which players can move freely in the field, and two teams compete against each other. For this kind of sports, each player's dominant region plays an important role to evaluate the teamwork. Therefore, here we propose some approaches to quantitative evaluation based on the concept of a generalized Voronoi diagram that divides space into dominant regions. We also construct a more realistic model of player's motion model based on experiments, and apply it to the evaluation.

28. Masahito Hayashi, Hiroshi Imai, Keiji Matsumoto, Mary Beth Ruskai, Toshiyuki Shimono:
“Qubit Channels which Require Four Inputs to Achieve Capacity: Implications for Additivity Conjectures”, ERATO Conference on Quantum Information Science (EQIS 2004), pp. 45–46, 2004 年 9 月.
概要: An example is given of a qubit quantum channel which requires four inputs to maximize the Holevo capacity. The example is one of a family of channels which are related to 3-state channels. The capacity of the product channel is studied and nu-

merical evidence presented which strongly suggests additivity.

29. Hisamoto Hiyoshi, Kokichi Sugihara:
"Improving the Global Continuity of the Natural Neighbor Interpolation", Computational Science and Its Applications-ICCSA-2004 (Lecture Notes in Computer Science), no. 3045, pp. 71–80, 2004年5月.
概要: The natural neighbor interpolation is a potential interpolation method for multidimensional data. However, only globally C^1 interpolants have been known so far. This paper proposes a globally C^2 interpolant, and write it in an explicit form. When the data are supplied to the interpolant from a third-degree polynomial, the interpolant can reproduce that polynomial exactly. The idea used to derive the interpolant is applicable to obtain a globally C^k interpolant for an arbitrary non-negative integer k. Hence, this paper gets rid of the continuity limitation of the natural neighbor interpolation, and thus leads it to a new research stage.

30. Tuyoshi Ito, Yuuya Sasaki, Hiroshi Imai, David Avis:
"Families of Tight Bell Inequalities Derived from Classes of Facets of Cut Polytopes", ERATO Conference on Quantum Information Science (EQIS 2004), pp. 78–79, 2004年9月.
概要: Recently triangular elimination method was proposed to convert facets of cut polytope to tight Bell inequalities in 2-party setting with many choices of 2-valued observables. In this paper, two formulas are presented which represent families of tight Bell inequalities. They result from applying triangular elimination to hypermetric and pure clique-web inequalities of cut polytope. In addition, we prove that under some conditions, the CHSH inequality is irrelevant given any one of the obtained Bell inequalities

31. Satoru Iwata, Satoko Moriguchi, Kazuo Murota:
"A Capacity Scaling Algorithm for M-convex Submodular Flow", 10th International IPCO Conference, pp. 352–367, 2004年6月.
概要: This paper presents a faster algorithm for the M-convex submodular flow problem, which is a generalization of the minimum-cost flow problem with an M-convex cost function for the flow-boundary, where an M-convex function is a nonlinear nonseparable discrete convex function on integer points. The algorithm extends the capacity scaling approach for the submodular flow problem by Fleischer, Iwata and McCormick (2002) with the aid of a novel technique of changing the potential by solving maximum submodular flow problems.

32. Deok-Soo Kim, Byunghoon Lee, Cheol Hyung Cho, Kokichi Sugihara:
"Plane-Sweep Algorithm of O(nlogn) for the Inclusion Hierarchy among Circles", Computational Science and Its Applications-ICCSA-2004 (Lecture Notes in Computer Science), no. 3045, pp. 53–61, 2004年5月.
概要: Suppose that we have a number of circles in a plane and some of them may contain some others. Then, finding the hierarchy among circles is of important for various applications such as the simulation of emulsion. In this paper, we present a plane-sweep algorithm which can identify the inclusion relationship among the circles in $O(n \log n)$ time in the worst-case. The algorithm uses a number of sweep-lines and a red-black tree for the efficient computation.

33. Shiro Matsuura, Kokichi Sugihara:
"Use of Discrete Topology for the Construction of Generalized Voronoi Diagrams", In-

ternational Symposium on Voronoi Diagrams in Science and Engineering, pp. 153–163, 2004年9月.

概要: This paper presents a new scheme for robust computation of generalized Voronoi diagrams, in which the robustness is guaranteed on the basis of topological consistency. The topology-based approach is one of the most successful principles for designing robust algorithms to solve geometric problems, which the author's group has been developed for a long time. This approach generates efficient algorithms because the floating-point arithmetic can be used, but is not a beginners' technique because topological invariants for individual problems are required in the design of the algorithms. The new scheme presented here uses discrete topology obtained from a digital-picture approximation of the Voronoi diagram. Hence, deep insight is not necessary to extract individual invariants. The basic idea together with its application to wire bundling is presented.

34. Masaki Moriguchi, Kokichi Sugihara:
"Isotropic and Feature-Preserving Mesh Simplification Based on Constrained Centroidal Voronoi Diagrams", International Symposium on Voronoi Diagrams in Science and Engineering, pp. 83–93, 2004年9月.

概要: We propose an efficient method for simplifying triangular meshes to isotropic and feature-preserved meshes. We first construct the constrained centroidal Voronoi diagram on the surface by using the Lloyd iteration method, and then we make the dual graph of it, i.e. the Delaunay triangulation, to obtain a simplified mesh. The constrained centroidal Voronoi diagram, whose centroids are constrained to the surface, is an extension of the 2D centroidal Voronoi diagram to surfaces in higher dimensions. By the nature of the centroidal Voronoi diagram, simplified meshes are highly isotropic; non-uniform mesh simplification (such as curvature-adapted one) can also be done by defining an appropriate density function over the surface. The distance is measured by the usual Euclidean distance, rather than the geodesic distance, and the constrained centroid is simply the closest point on the surface to the unconstrained centroid. This property makes it easier to construct the constrained centroidal Voronoi diagram. Finally further constraining some centroids to the surface features (sharp edges, user-defined edges, boundary edges, etc.), we could achieve feature-preserving mesh simplification.

35. Kazuo Murota:
"Fundamentals in Discrete Convex Analysis", Dagstuhl Seminar, Computing and Markets, 2005年.

概要: This talk describes fundamental properties of M-convex and L-convex functions that play the central roles in discrete convex analysis. These concepts were originally introduced in combinatorial optimization, but turned out to be relevant in economics. Emphasis is put on discrete duality and conjugacy respect to the Legendre-Fenchel transformation.

36. Kohei Murotani, Kokichi Sugihara:
"Watermarking 3d Polygonal Meshes Using Generalized Singular Spectrum Analysis", NICOGRAPH International Conference 2004, pp. 121–126, 2004年.

概要: This paper presents a generalization of the singular spectrum analysis (SSA) and applies it to the construction of a new robust watermarking method that adds a watermark to a 3D polygonal mesh in the spectral domain. The basic SSA is a fundamental tool for analyzing one-dimensional sequence such as time series, and is not suitable for multi-dimensional data. In order to overcome this difficulty, we generalize the

basic SSA in such a way that it can be used for the 3D polygonal meshes. Watermarks embedded by this method are resistant to similarity transformations and random noises.

37. Tetsushi Nishida, Kokichi Sugihara:
"Extended Fast Marching Method for the Boat-Sail Distance and Its Applications", Mathematical Aspects of Image Processing and Computer Vision 2004, 2004年11月.
概要: In this talk, we introduce a boat-sail distance. Suppose that we want to travel on the surface of water with a boat. If there is no flow of water, the boat can move in any direction at the same maximum speed. If the water flows, on the other hand, the speed of the boat is anisotropic; the boat can move faster in the same direction as the flow, while it move only slowly in the direction opposite to the flow direction. Thus, a boat-sail distance is defined as the smallest time necessary for the boat to move from one point to another. According to this distance, the surface of water is partitioned into regions. This partition is called a boat-sail Voronoi diagram.

38. Tetsushi Nishida, Kokichi Sugihara:
"Approximation of the Boat-Sail Voronoi Diagram and Its Application", International Symposium on Voronoi Diagrams in Science and Engineering, pp. 63–72, 2004年9月.
概要: A new generalized Voronoi diagram, called a boat-sail Voronoi diagram, is defined on the basis of the time necessary for a boat to reach on water surface with flow. The problem of computing this Voronoi diagram is reduced to a boundary value problem of a partial differential equation, and a numerical method for solving this problem is constructed. The method is a modification of a so-called fast marching method originally proposed for the eikonal equation. Computational experiments show the efficiency and the stableness of the proposal method. We also apply our equation to the simulation of the forest fire.

39. Tetsushi Nishida, Kokichi Sugihara:
"Boat-Sail Voronoi Diagram on a Curved Surface", International Symposium on Voronoi Diagrams in Science and Engineering, pp. 63–72, 2004年9月.
概要: We propose a new generalized Voronoi diagram, called a "boat-sail Voronoi diagram on a curved surface". This is an extention of the boat-sail Voronoi diagram. The boat-sail Voronoi diagram is the partition of a two-dimensional plane, on the basis of the boat-sail distance. On the other hand, our new Voronoi diagram subdivides the curbed surface with flow into the regions. In this paper, we derive a partial diffrential equation to solve the boat-sail Voronoi diagram on a curved surface and show some numerical examples.

40. Mayumi Oto, Hiroshi Imai, Keiko Imai, Toshiyuki Shimono:
"Computational Geometry of Bloch Sphere", ERATO Conference Quantum Information Science 2004 (EQIS2004), pp. 156–157, 2004年9月.
概要: On the Bloch sphere, computational-geometric problems can be treated for the quantum divergence as a proximity function, whose geometry is called quantum information geometry. By generalizing the result by Onishi and Imai on the computational-geometric structure in the classical information geometry, where the Kullback-Leibler divergence is used as a proximity function, Voronoi diagrams are introduced. We show the minimum enclosing sphere problem with respect to the quantum divergence is related to the approximate computation of the Holevo capacity of a quantum communicatin

channel,and based on an assumption it produces n-approximate solution in time $O(1/n)$.

41. Mayumi Oto, Hiroshi Imai, Keiko Imai:
"Computational Geometry on 1-qubit Quantum States", International Symposium on Voronoi Diagrams in Science and Engineering, pp. 145–151, 2004 年 9 月.
概要: A set of 1-qubit quantum states are represented by a unit sphere, called the Bloch sphere. On the Bloch sphere, computational-geometric problems can be treated for the quantum divergence as a proximity function, whose geometry is called quantum information geometry. By generalizing the result by Onishi and Imai on the computational-geometric structure in the classical information geometry, where the Kullback-Leibler divergence is used as a proximity function, Voronoi diagrams are introduced. The minimum enclosing sphere problem with respect to the quantum divergence is related to the approximate computation of the Holevo capacity of a quantum communication channel, and based on an assumption observed by experiments it produces ϵ-approximate solution in time $O(1/\epsilon)$.

42. Kokichi Sugihara:
"Robust Geometric Computation Based on Digital Topology", Proceedings of the 10th International Computing and Combinatorics Conference (Computing and Combinatorics, Lecture Notes in Computer Science), no. 3106, pp. 3–12, 2004 年 8 月.
概要: This paper present a new scheme for designing numerically robust geometric algorithms based on topological consistency. The topology-based approach is one of the most successful principle for designing robust algorithms to solve geometric problems, which the author's group has been developed for a long time. This approach generates efficient algorithms because the floating-point arithmetic can be used, but is not a beginners' technique because topological invariants for individual problems are required in the design of the algorithms. The new scheme presented here uses digital topology instead of individual invariants, and hence will change the topology-based approach from a middle-level technique to a beginners' level technique. The basic idea together with its application to wire bundling is presented.

43. Kokichi Sugihara:
"Realization of Impossible Objects and a New Type of Visual Illusion", Mathematical Aspects of Image Processing and Computer Vision 2004, 2004 年 11 月.
概要: There is a class of line drawings called "pictures of impossible objects", which give us some impression of three-dimensional solid objects but at the same time give us impression that such objects cannot be realized. These pictures are familiar in the sense that famous artists such as Escher used these pictures for their artwork. It is usually believed that the solid structures represented in these pictures cannot be realized as three-dimensional objects. However, some of pictures of impossible objects actually represent three-dimensional solid objects. Those pictures can be identified by the theory of interpretation of line drawing, which has a long history in computer vision. In this talk we focus on the way of reducing the realizability of objects to the feasibility of linear constraints, together with some combinatorial aspects of the problem in order to reduce the time complexity as well as to circumvent numerical instability.

研究会等

1. David Avis, 今井浩, 伊藤剛志, 佐々木勇也
:

“非線形および半定値計画を用いたBell不等式の必要性関係の判定”, 第11回 電子情報通信学会量子情報技術研究会（QIT11）, 2004年12月.

概要: Bell不等式は量子状態の非局所性を捉える道具として重要である．CollinsとGisinはCHSH不等式を満たしI_3322 Bell不等式を破る量子状態の存在を示した．この性質はCHSH不等式に対するI_3322不等式の必要性と呼ばれる．I_3322不等式に対して必要性を持つBell不等式の例は知られていない．本論文では非線形最適化を繰り返し用いてBell不等式の必要性を判定する方法を提案し，これによっても同じ結果を導けることを示す．提案方法では量子状態がCHSH不等式を満たす必要十分条件であるHorodecki条件を用いていないため，他のBell不等式のI_3322不等式に対する必要性を調べるのにも適用できる．さらに半定値計画を組み合わせた方法も提案し，両方法の現時点での問題点を述べる．

2. 林正人，今井浩，松本啓史，Mary Beth Ruskai, 下野寿之:
“ホレボ容量の加法性 －最適信号数4を持つ量子ビットチャンネルの考察から－”, 第10回 電子情報通信学会量子情報技術研究会（QIT10）, 2004年5月.

概要: An example is given of a qubit quantum channel which requires four inputs to maximize the Holevo capacity. The example is one of a family of channels which are related to 3-state channels. The capacity of the product channel is studied and numerical evidence presented which strongly suggests additivity. The numerical evidence also supports a conjecture about the concavity of output entropy as a function of entanglement parameters. However, an example is presented which shows that for some channels this conjecture does not hold for all input states.

3. Hiroshi Hirai, Kazuo Murota, Masaki Rikitoku:
“Electric Network Kernel for Support Vector Machines”, 日本オペレーションズ・リサーチ学会2005年度春季研究発表会, 2005年3月.

概要: This paper investigates support vector machine (SVM) with a discrete kernel, named electric network kernel, defined on the vertex set of an undirected graph. Emphasis is laid on mathematical analysis of its theoretical properties with the aid of electric network theory and the theory of discrete metrics. SVM with this kernel admits physical interpretations in terms of resistive electric networks; in particular, the SVM decision function corresponds to an electric potential. Preliminary computational results indicate reasonable promise of the proposed kernel in comparison with the Hamming and diffusion kernels.

4. 今井浩:
“量子情報処理一時世代モデルの新展開”, 第３回情報科学技術フォーラム（FIT2004）, 2004年9月.

概要: 量子コンピュータは，暗号セキュリティの諸問題を極めて効率的に解けることが理論的に示されたことによって，次世代計算モデルとして期待されている．これらは，量子力学原理を情報処理に活用するものであるが，量子力学というところがとっつきにくかったりする．本稿では，そのようなある種の壁を乗り越えて，量子コンピュータ研究が今のコンピュータ科学の延長線上にもあることを簡明に解説することを試みる．

5. 岩田覚，清水亮:
“行列束のKronecker標準形の組合せ論的解析”，日本応用数理学会年会，pp. 398–399, 2004年9月.

概要: 微分代数方程式で記述される動的システムの解析においては, 行列束のKronecker標準形の構造指数が基本的な役割を果たしている．しかし, 構造指数は, 摂動に対して不安定な離散値を取るため, 正確に計算するには, 計算誤差に対してロバストな手法の開発が必要とされる. 本研究は, 行列束の零非零

構造に注目し, 数値誤差の生じ得ない組合せ的手法によって構造指数の精密な推定値を計算することを目的としている.

6. 垣村尚徳, 岩田覚:
“符号対称行列の Sylvester 指数”, 日本ＯＲ学会秋季研究発表会, pp. 228–229, 2004 年 9 月.
概要: 各要素の符号情報が与えられた対称行列は, 非零要素の絶対値によらず, 常に正則であることが保証されるとき, 符号正則といわれる. 符号正則な対称行列においては, その Sylvester 指数が一意に定まることが知られている. 本研究では, 符号正則な対称行列の符号指数を具体的に計算する効率的なアルゴリズムを設計した. また, 与えられた対称行列の Sylvester 指数が符号情報のみから決定不可能であることを判定する問題が NP 完全であることを示した.

7. 森口聡子, 室田一雄:
“L 凸関数に対する離散ヘッセ行列”, 日本ＯＲ学会 2005 年度春季研究発表会, 2005 年 3 月.
概要: L 凸関数は, 整数格子点上で定義された関数のクラスとして, 離散凸解析において中心的な役割を担っている. 本稿では, L 凸関数に対して, 離散ヘッセ行列と局所 2 次展開を定義し, これらを用いて L 凸関数の特徴付けを行う.

8. Kazuo Murota:
“DE vs IMT: Some History and Some Mathematics”, 京都大学数理解析研究所研究集会「Thirty Years of the Double Exponential Transforms」, 2004 年 9 月.
概要: Comparison is made between the Double Exponential formula and the IMT rule for numerical integration in terms of basic ideas, error estimates, and optimality. This talk is intended to be a kind of personal recollection of an applied mathematician who had the fortune to work on this topic as the first research subject in his career and, since then, witnessed the subsequent continual developments as a passive onlooker.

9. Tetsushi Nishida, Kokichi Sugihara:
“Robust Numerical Method for the Boat-Sail Distance and Its Applications”, 第 33 回数値解析シンポジウム, pp. 65–68, 2004 年 5 月.
概要: Suppose that we want to travel on the surface of water with a boat. If there is no flow of water, the boat can move in any direction at the same maximum speed. If the water flows, on the other hand, the speed of the boat is anisotropic; the boat can move faster in the same direction as the flow, while it move only slowly in the direction opposite to the flow direction. Modeling this situation, we can introduce the boat-sail distance. In order to construct a numerical method for computing the boat-sail distance, we reduce the problem to a boundary value problem of a partial differential equation. This idea is the same as the idea for reducing the problem of computing the Euclidean distance to a boundary value problem of the eikonal equation. Hence, our formulation can be considered a generalization of the eikonal equation. In the case of the eikonal equation, the fast marching method is well known as an efficient and stable computational technique. Therefore we applied the idea of the fast marching method to our equation, but we found that it did not work well. In this paper, we propose a new method by extending the scheme of the fast marching method and show the efficiency and the stableness of the proposal method by numerical experiments.

10. Tetsushi Nishida, Kokichi Sugihara:
“FEM-like Fast Marching Method for the Computation of the Boat-Sail Distance”, 情報処理学会研究会研究報告, pp. 105–112, 2004 年 1 月.
概要: 流れのある水面上を航行するボートの

振舞いをモデル化することによって，ボート航行距離という概念を導入する．そして，この距離を計算する問題を偏微分方程式の境界値問題に定式化し，得られた境界値問題を解く数値計算法を構成する．その方法はeikonal方程式に対して提案されたfast marching法を改良したものである．数値実験により，提案した方法が効率性よく安定に動作することを示す．

11. 大音真由美, 今井浩, 今井桂子:
“１量子ビットの量子状態における計算幾何とその応用”, 第 11 回量子情報技術研究会 (QIT11), pp. 121–126, 2004 年 12 月.
概要: Let a parameter space of qubits be the quantum state space. In this space, computational-geometric problems can be treated for the quantum divergence as a proximity function, whose geometry is called quantum information geometry first researched by Nagaoka. By generalizing the result by Onishi and Imai on the computational-geometric structure in the classical information geometry, where the Kullback-Leibler divergence is used as a proximity function, Voronoi diagrams are introduced. We describe the farthest Voronoi diagram in quantum information geometry, and the minimum enclosing sphere problem in the quantum state space of 1-qubit.

12. 大音真由美, 今井浩, 今井桂子:
“計算幾何を用いた 1 量子ビットの量子通信における Holevo 容量計算のアルゴリズム”, 情報処理学会アルゴリズム研究会, pp. 115–119, 2004 年 10 月.
概要: 量子ビットで表現されるパラメータ空間を量子空間と定義したとき，この量子空間における計算幾何では，量子ダイバージェンスは近傍関数として扱うことができ，量子計算幾何と呼ばれている．本研究は，大西と今井による古典情報幾何での計算幾何学的構造の研究成果を量子情報幾何に拡張したものであり，ここではKullback-Leiblerダイバージェンスは近傍関数として用いられており，ボロノイ図が導入されている．本稿ではまず，1 量子ビットの量子空間における最小包含球問題について述べ，その応用として量子通信路でのホレボ容量を計算するアルゴリズムを提案する．次に，量子空間の離散化によって時間計算量が $O(1/\epsilon)$ で ϵ 近似解を持つことを述べる．

13. 佐々木勇也, 伊藤剛志, 今井浩, David Avis:
“組合せ論から導出される Bell 不等式”, 第 10 回 電子情報通信学会量子情報技術研究会（QIT10）, 2004 年 5 月.
概要: Bell 不等式，特にタイトなものを求める研究がここ数年で進んできている．本発表では，組合せ論でのカット凸多面体の理論を適用して，2 パーティ，m 観測量，2 観測値の場合においてカット多面体のファセットから新しく Bell 不等式を導出する手法について概説し，特にその不等式がタイトであり互いに本質的に異なることを示す．結果として，2 パーティ，10 観測量，2 観測値のタイトで互いに異なる Bell 不等式を CHSH 不等式以外に 44,368,793 種類発見することに成功した．

14. 谷口隆晴，杉原厚吉:
“非粘性圧縮流体方程式に対する方向適合型無反射境界条件”, 第 33 回数値解析シンポジウム講演予稿集, pp. 13–17, 2004 年.
概要: 数値流体力学をはじめとする現実問題を取り扱った数値計算では，広大な現実の空間に比べ計算機の中で扱うことのできる領域は高々有限であり，計算対象となる空間の打ち切りが必要となる．このとき，打ち切られた断面という人工的な境界が生じてしまうが，そのような人工的な境界上では特別な取り扱いをしない限り，現実には存在しない反射波が生成されてしまう．そこで，境界上で反射波をなくすような境界条件，すなわち無反射境界条件の設定が必要となる．無反射境界条件は既にいくつか提案されているが，既存の手法では波が境界に対して垂直に入射する，という仮定がおかれていた．本発表では，非粘性圧縮流体方程式 (Euler 方程式) を考え，解が境界付近で単純波として挙動する，

という仮定をおくことによって，流れが垂直という仮定を持たない無反射境界条件を提案する．

15. 谷口隆晴，杉原厚吉:
“特性曲線法を用いた新しい無反射境界条件”, 日本流体力学会年会 2004, G-221, 2004 年.
概要: Because the computational resources are finite, one needs to truncate the computational domain when he/she simulates a physical problem. This truncation gives rise to non-physical artificial boundaries. Practically nonreflecting boundary conditions, which are boundary conditions that prevent the generation of reflections, are of great importance. One of the most popular methods for the Navier-Stokes equations right now is boundary condition by Poinsot and Lele boundary conditions. However, their method is based on Thompson's boundary condition for the Euler equations, which is essentially one-dimensional, and hence is valid only when the flow is perpendicular to the boundary. Here we propose a boundary condition for the Navier-Stokes equations which does not require the assumption for the direction of flow. Our basic idea is to estimate the direction of the flow with numerical data.

16. 谷口隆晴，杉原厚吉:
“特性曲線法に基づく無反射境界条件の提案とその実装法”, 第 18 回数値流体力学シンポジウム, B2-3, 2004 年.
概要: A characteristic nonreflecting boundary treatment is presented. Because the computational resources are finite, one needs to truncate the computational domain when he/she simulates a physical problem. This truncation gives rise to non-physical artificial boundaries. Practically nonreflecting boundary conditions are employed to eliminate non-physical reflections on such boundaries. One of the most often-used methods right now is Poinsot–Lele boundary conditions which, however, have an assumption that the incident waves are perpendicular to the boundaries. To overcome this restriction, we have proposed a characteristic boundary condition for the Navier-Stokes equations which does not have the assumption for the direction of the flow; however, how to implement this condition is not so trivial. Here we propose a method to implement our boundary condition. The method presented here is derived to guarantee the numerical robustness and the symmetric property of the solutions.

17. 山田崇， 由良文孝， 今井浩:
“Schrodinger の「車」: 交通流セルオートマトンの量子化”, 第 11 回　電子情報通信学会量子情報技術研究会（QIT11）, pp. 115–119, 2004 年 12 月.
概要: 1 次元セルオートマトンによる交通流モデルの量子版を提案する．Watrous の定義した 1 次元量子セルオートマトンでは条件が厳しいため，遷移の条件を緩和した上でモデルを考える．結果，古典セルオートマトン上での交通流モデルでみられる渋滞といった交通流ならではの現象を今回提案した量子交通流モデルでも再現し，状態の重ね合わせを制御することにより流量を相転移的に変化させられることを示した．

C03: ネットワーク上での社会的効用と個人的効用の対立問題に対するアルゴリズム的研究

浅野 孝夫

中央大学 理工学部 情報工学科
〒 112-8551 文京区春日 1-13-27
asano@ise.chuo-u.ac.jp

1 はじめに

計算理論・アルゴリズム理論の代表的問題の一つである集合カバー問題は、社会学・経済学にも関係して、サービスの提供と利用という形で説明できる問題である。一般に、サービスを提供する事業者は負担したコストをこのサービスの受益者から回収することになるが、その際どのように受益者にコストを負担してもらうかということになる。サービスを開業した複数の事業者からサービスが受けられる状況のときには、利用者は負担が軽くなる事業者からのサービスを希望するようになる。こうして利用者が利己的に行動をするようになると、開業した事業者は、開業のコストを回収できなくなり、このシステムは破綻に向かって進んでいくことになってしまう。これに対して、どの利用者も、他の利用者の負担金をそのままにしておいて、勝手に自分の負担金を減らすとサービスが受けられなくなってしまうとき、このときの状態はゲーム理論の専門用語で Nash 均衡にあると呼ばれる。Nash 均衡を求めるための計算困難性や近似困難性の上界・下界の研究が活発に実行されていて、現在、情報科学の世界的な権威の国際会議では、この分野の研究がホットなトピックスとして注目を浴びている。

上記のような研究動向を踏まえて、本研究は、集合カバー問題、施設配置問題 (集合カバー問題と類似する問題であるが、各受益者はサービスを提供する施設の開設コストを負担するだけでなくサービスを受け取るための接続コストも支払うという問題)、インターネットの回線利用問題、通信網 (道路網) の混雑による遅延対策問題、などの NP-困難な組合せ最適化問題に対して、利己的な利用者と全体の管理者との間の対立問題をアルゴリズムの観点から研究し、計算困難性・近似困難性のより良い下界と上界を得ることを目的としている。

ネットワーク上での全体からの社会的効用の最適化と利己的な各利用者の納得できる個人的効用の達成という対立問題は、問題の下界を証明する際にもしばしば生じる問題で、情報科学の分野ではなじみの問題である。さらに、実際の現場で生じる全体と個との対立の観点からの問題は、NP-困難な組合せ最適化問題であり、整数計画問題として定式化できるものが多い。このような問題に対しては、近似アルゴリズムの理論が強力な道具である。以上を踏まえて、以下の研究を実行した。

1. インターネットや道路網などで社会的効用の最適化と利己的な各利用者の納得できる個人的効用の達成という対立問題の生じる実際の具体例とこれまでの研究を調査した。

2. ゲーム理論や社会学、経済学で扱われている全体と個の対立問題の Nash 均衡に基づく理論的研究を調査した。

3. 集合カバー問題、施設配置問題などの NP-困難な組合せ最適化問題に対して開発された近似アルゴリズムの設計と解析の技法が、本研究に有効であることが既に知られている。そこで、1,2 の調査においては、高性能近似アルゴリズムの分野で最先端の研究をしている内外の研究者と情報およびアイデアを交換した。

4. 1,2,3 の研究調査で得られた問題および集合カバー問題、施設配置問題、インターネットの回線利用問題、通信網 (道路網) の混雑による遅延対策問題などの、NP-困難な組合せ問題に対して、利己的な利用者と全体の管理者との間の対立問題

を近似アルゴリズムの観点から研究した。また、近似アルゴリズムの設計と解析の技法の有効性を検討中である。

以上の研究を通して得られた成果は、研究業績一覧に載せているが、その中の１つを以降の節で詳しく述べる。

2 合流フローの混雑最小化アルゴリズムに対する実験的性能評価と貪欲改善

2.1 序論

ネットワーク・フローの中で,「すべての点においてフローが出て行く辺が 1 本以下」という条件を満たすものを**合流フロー** (confluent flow) という．現実社会において，合流フローとなる例は数多く存在する．いくつかの例を以下に挙げる．

- **インターネット・ルーティング:** インターネットにおける多くのルータは，宛先の情報 (IP アドレスやネットワークアドレス) だけを利用してルーティングを行っている．そこで，宛先が同一のパケットの流れを抜き出すと，合流フローになる．

- **CDN:** CDN (content delivery network, コンテンツ配信ネットワーク) におけるデータは，オリジナルの配信サーバから各 ISP (Internet service provider) のキャッシュサーバを経てクライアントへと送られる．このデータの流れを逆向きにすると，合流フローになる．

- **避難経路:** ビルやホテルなどの各フロアには非常口誘導灯があり，多くの場合，非常口までの最短経路を示す一方向の矢印がついている．建物内の人が一斉に避難するとき，人の流れは合流フローになる．

他の合流フローの例には，ブロードキャスト・マルチキャストにおけるデータの流れなどがある．

ここでは，まず問題定義を行い，Chen et al. の手法 [1] と提案手法について述べたあと，それらの手法に対する実験的性能評価を行う．

2.2 問題定義

$G = (V, E)$ を有向グラフとし，各点の**需要** (demand) を $d : V \to \mathbb{R}_+$ とする．本論文では G の点数 $|V|$ を n，辺数 $|E|$ を m と表す．また，k 個の**シンク** (sink(s)) を $S = \{s_1, \ldots, s_k\} \subset V$ とし，各シンクの出次数 (out-degree) は 0 であるとする．需要をシンクに流すフロー $f : E \to \mathbb{R}_+$ は，各点 $v \in V - S$ において，フロー保存則

$$\sum_{e=(v,w)\in E} f(e) - \sum_{e=(u,v)\in E} f(e) = d(v)$$

を満たす．また，各点 v において

$$\mathrm{in}(v) = \sum_{e=(u,v)\in E} f(e)$$

としたとき，フロー f の点 v における**混雑** (congestion) を

$$c(v) = d(v) + \mathrm{in}(v), \tag{2.17}$$

フロー f の混雑を

$$\max_{v\in V} c(v) \tag{2.18}$$

と定義する．

合流フローは連結成分 $\{T_1, \ldots, T_k\}$ からなる G の部分グラフになり，各連結成分 T_i は根 s_i に向かう有向木になる．T_i において混雑が最大となる点はシンク s_i であり，その混雑は T_i に含まれる点の需要の合計である (これを $d(T_i)$ と表す)．このとき，フローの混雑は

$$\max_{i=1,\ldots,k} d(T_i) \tag{2.19}$$

となる．

本論文で扱う**合流フローの混雑最小化問題** (congestion minimization confluent flow problem) の目的は，フローの混雑が最小となる合流フローを求めることである．この問題は，NP-困難な点素パス問題 (vertex-disjoint path problem) からのリダクションにより，近似率を $\frac{1}{2}\log_2 k$ より良くすることは NP-困難であることが証明されている [1].

合流フローの概念は 1999 年に発表された Kleinberg, Rabani and Tardos [5] の一部で述べられ

ている．本論文で扱う合流フローの混雑最小化問題は，2003 年に Chen, Rajaraman and Sundaram [2] によって定義されたものであり，[2] ではランダム・ラウンディングを使用した $O(\log^3 n)$-近似アルゴリズム (最適な分割可能フローの混雑を 1 とおいて) が提案されている．また，2004 年には Chen et al. [1] によって $(1+\log_2 k)$-近似，$(1+\ln k)$-近似の決定性アルゴリズムが提案されている．合流フロー問題は新しい問題であり，今後，研究が進んでいくと思われる．

近似率の下界

合流フローに似た概念として，分割不可能フロー (unsplittable flow) がある．分割不可能フローとは,「各点の需要を 1 本のパスで流さなければならない」という制約がついたものである．分割不可能フローの混雑最小化問題に対しては Kleinberg [4] や Dinitz, Garg and Goemans [3] によって定数近似アルゴリズムが与えられている．また，これらの制約がなく，自由に分けて流してよいものを分割可能フロー (splittable flow) という．混雑が最小となる分割可能フローは，多項式時間で求めることができる．

本論文では，合流フローの混雑の下界として，分割可能フローを用いる．分割可能フローの最適解が，合流フローの最適解以下となるのは明らかである．Chen et al. [1] において，分割可能フローと合流フローの間のギャップが H_k となる例が示されている．

2.3 Chen et al. (2004) のアルゴリズム [1]

この節では，Chen et al. の $(1+\log_2 k)$-近似アルゴリズムと $(1+\ln k)$-近似アルゴリズムについて述べる．$(1+\ln k)$-近似アルゴリズムは，$(1+\log_2 k)$-近似アルゴリズムの一部を変更したものである．

準備: まず，混雑が最小となる分割可能フロー f を求め (容量を 2 分探索により変化させて最大フローアルゴリズムを適用し，すべての点の需要を流しきることができる最小の容量を求める)，その混雑が 1 となるように，各点の需要と各辺のフローを一様にスケーリングする．このとき，フローが流れない辺をグラフから削除する．最大フローは有向閉路が存在しないようにできるので，このグラフは有向無閉路グラフと仮定できる．この有向無閉路グラフにおいて，シンクに隣接する各点を**境界点** (frontier node) という．また，アルゴリズムが開始されるとき，すべてのシンクは活性であるとする．

$(1+\log_2 k)$-近似アルゴリズム

下記の 1, 2, 3 の条件を順に判定し，一番はじめに条件を満たした操作を行う．

main loop: $|V(G)| > k$ の間，以下を実行する．

1. **node aggregation:** 境界点 v を始点とするすべての辺の終点が同一のシンク s_i のとき，その中の 1 本をマークし，v を s_i に縮約する．さらに，$d(v)$ を $d(s_i)$ に加え，main loop に戻る．

2. **breaking sawtooth cycle:** グラフ G における境界点からシンクへの各辺 $e=(v,s)$ に対して，逆辺 $e_{\mathrm{rev}}=(s,v)$ を付加したグラフを $\hat{G}$ とする．$\hat{G}$ が長さ 3 以上の単純有向閉路 C を持つとき f を以下のように更新する．$C \cap E(G)$ の辺におけるフローの最小値を $f_{\min}$ とする．G の各辺 e について，$e \in C$ ならば $f(e) := f(e) - f_{\min}$ とし，$e_{\mathrm{rev}} \in C$ ならば $f(e) := f(e) + f_{\min}$ とする．フローが 0 の辺をすべて削除し，main loop に戻る．

3. **sink deactivation:** 隣接する境界点が 1 つであるシンクを s_j とする．s_j に隣接する境界点を v，v に隣接する s_j 以外の任意のシンクを s_ℓ とする．このとき，$c(s_j)+f(v,s_\ell) < c(s_\ell)-f(v,s_\ell)$ ならば辺 (v,s_ℓ) を削除し，そこを流れるフローを (v,s_j) に流す．そうでないとき，辺 (v,s_j) を削除し，そこを流れるフローを (v,s_ℓ) に流して，s_j を不活性にする．その後，main loop に戻る．

output: マークされた辺を出力する．

1, 2 の条件を満たさない場合，境界点とシンクを結ぶすべての辺で誘導される G の (単純) 部分

グラフは，向きを無視すると森になる．辺がある限り，この森には次数 1 の点が存在し，それが 3 の条件を満たすシンク s_j となる．

$(1+\ln k)$-近似アルゴリズム

$(1+\log_2 k)$-近似アルゴリズムの sink deactivation を以下のように変更する．

3. **parsimonious sink deactivation:** 以下の条件を満たす $G_1 \subseteq G$ を求める:
   - G_1 の各辺は境界点とシンクを結ぶ (G_1 は 2 部グラフになる)．
   - 境界点 v が G_1 に含まれるとき，v を始点とする G の辺はすべて G_1 に含まれる (したがって v から他の境界点に向かう G の辺はない)．
   - シンク s が G_1 に含まれるとき，s を終点とする G の辺はすべて G_1 に含まれる．
   - 各境界点は 2 つ以上のシンクに隣接している．

   G_1 に含まれるシンクの集合を S_1 と表す．G_1 に対して以下の操作を行う．
   i. **balancing:** G_1 において，$\sum_{s_i \in S_1} \mathrm{e}^{c(s_i)}$ が最小となるように各辺のフローを再分配し，フローが 0 となった辺を削除する．
   ii. $\mathrm{in}(s)$ が最小となるシンク $s \in S_1$ を求める．s に隣接する各境界点 v に対して，辺 (v,s) を流れるフローを v が隣接する他の任意のシンクに流し，辺 (v,s) を削除する．s を不活性にし，$S_1 := S_1 - \{s\}$ とする．
   iii. **balancing** を行い，main loop に戻る．

G_1 は以下のように求める．$\hat{G}$ を強連結成分分解し，各強連結成分を点とする有向無閉路グラフにおいて，出次数が 0 となる点集合が G_1 である．

次に，$\sum_{s_i \in S_1} \mathrm{e}^{c(s_i)}$ の最小化を考える．G_1 における境界点の集合を F_1 とする．また，辺 e を流れるフローを x_e と表すとき，balancing における $\sum_{s_i \in S_1} \mathrm{e}^{c(s_i)}$ の最小化は，以下の凸計画 (convex programming) 問題として定式化できる．ここで，y_s はシンク s の混雑を表す変数である．

$$\min \quad \sum_{s \in S_1} \mathrm{e}^{y_s} \tag{2.20}$$

$$\text{s.t.} \quad \sum_{e=(v,w) \in E(G_1)} x_e \geq c(v) \qquad (v \in F_1)$$

$$y_s \geq \sum_{e=(u,s) \in E(G_1)} x_e + d(s) \ (s \in S_1)$$

$$x_e \geq 0 \qquad (e \in E(G_1))$$

制約式中の $c(v)$ は，G における点 v の混雑を表す．また，凸計画問題は，多項式時間で最適解を求めることができる [6, 7].

解析の概要

node aggregation と breaking sawtooth cycle を行ったとき，どの点においても混雑が増加せず，少なくとも 1 本の辺が減少する．

sink deactivation と parsimonious sink deactivation の解析にはポテンシャル関数を用いる．シンク s_i のポテンシャルを

$$\phi(s_i) = 2^{c(s_i)} \tag{2.21}$$

とし，フローのポテンシャルを活性なシンクのポテンシャルの合計とする．このとき，sink deactivation を行ってもフローのポテンシャルは増加しない．アルゴリズムが開始されるとき，各シンクのポテンシャルは高々2 であり (各点の混雑は高々1 なので)，フローのポテンシャルは $2k$ 以下となる．sink deactivation を行ったあともこの値は増加しないので，アルゴリズム終了時の各シンクのポテンシャルは $2k$ 以下であり，各シンクの混雑が $1+\log_2 k$ $(=\log_2(2k))$ 以下となる．

次にポテンシャル関数を

$$\phi(s_i) = \mathrm{e}^{c(s_i)} \tag{2.22}$$

と変更する．このとき，parsimonious sink deactivation を行ってもフローのポテンシャルは増加しない．よって各シンクのポテンシャルは $\mathrm{e}k$ 以下となるので，アルゴリズム終了時の各シンクの混雑は $1+\ln k$ 以下となる．

2.4 提案手法

Chen et al. のアルゴリズムで得られた解に対して，貪欲改善を行うと性能が大きく向上する．この節では，本論文で提案する手法について述べる．提案手法は，与えられた合流フローに対して，フローを流す辺を 1 本変えたときの混雑を求め，それが最小となるように解を変更していくものである．

与えられた合流フローにおいて，$d(T_i)$ が最大となる連結成分の集合を $T_{\max} \subseteq \{T_1, \ldots, T_k\}$ と表す (混雑が最大となるものが複数存在する場合もある)．このとき，本論文において提案するアルゴリズムを以下に述べる．

1. $u \in T_{\max}$, $v \notin T_{\max}$ となる各辺 $e = (u, v) \in E(G)$ に対して，点 u からのフローを辺 e に流したときのフローの混雑 (これを $r(e)$ と表す) を計算する．
2. $r(e)$ が最小となる辺 $e_{\min}$ を求める．
3. 現在のフローの混雑を $cong$ としたとき，$cong > r(e_{\min})$ ならば，合流フローを辺 $e_{\min}$ に変更して，1 へ戻る．$cong \leq r(e_{\min})$ ならば現在のフローを出力する．

実験的性能評価

方法

本論文では，以下の 5 手法の比較を行った．

A. $(1 + \log_2 k)$-近似アルゴリズム

B. $(1 + \ln k)$-近似アルゴリズム

C. $(1 + \log_2 k)$-近似アルゴリズムで得られた解を初期解として，提案手法を適用

D. $(1 + \ln k)$-近似アルゴリズムで得られた解を初期解として，提案手法を適用

E. 各点の需要を最も近いシンクに流す合流フローを初期解として，提案手法を適用

近似率の下界には，混雑最小の分割可能フローを用いる (2.2 節参照)．また，各点数，辺数，シンク数に対して，1,000 個のインスタンスを生成し，それらを A から E のすべての手法で解いた．実験で使用した計算機環境は以下の通りである．

CPU	Intel Pentium4 1.7 GHz
メモリ	1,024 MB RDRAM
OS	Red Hat Linux 7.3
コンパイラ	g++ 2.96

結果

シンク数を変化させた場合　まず，点数・辺数を固定し，シンク数を変化させた．図 2.1 は，点数を 200，辺数を 1,000 として，シンク数を変化させた場合の近似率の平均である．各点の需要は一様乱数で与えた．どの手法を用いた場合にも，シンク数が 100 のときに最も悪い結果となった．シンクが少ない場合や多い場合には，提案手法の結果が非常に良くなったが，シンク数が 100 付近では，従来手法との差が小さくなった．点数を 100, 300 として同様の実験を行ったところ，どちらの場合もシンク数が点数のちょうど半分のときに全手法で最悪の結果となり，従来手法と提案手法の性能差も小さくなった．

この原因を調べるために，最適解との比較を行った．大きなインスタンスに対して最適解を求めるのは困難なので，点数 10，辺数 20 のグラフに対してシンク数を変化させる．結果を図 2.2 に示す．グラフは分割可能フローの混雑を 1 としたときの，最適解 (OPT)，手法 B, D の解の平均である．シンク数が点数の半分のときに，下界 (分割可能フロー) と最適解の間のギャップが大きくなっており，最適解と手法 B, D の間には，シンク数による混雑の変化は見られなかった．大きなインスタンスにおいても，同様のことが予想できる．また，点数に対するシンクの割合が等しい場合には，以下のように点数が多い (つまりシンク数が多い) 場合の方が近似率が悪くなる．

インスタンス			近似率 (平均)	
n	m	k	B	D
100	500	50	1.554324	1.527063
200	1,000	100	1.608197	1.564448
300	1,500	150	1.638836	1.588455

辺数を変化させた場合　次に，点数を 200，シンク数を 20 に固定して辺数 (辺の密度) を変化させた (図 2.3)．点数に対するシンクの割合が小さい

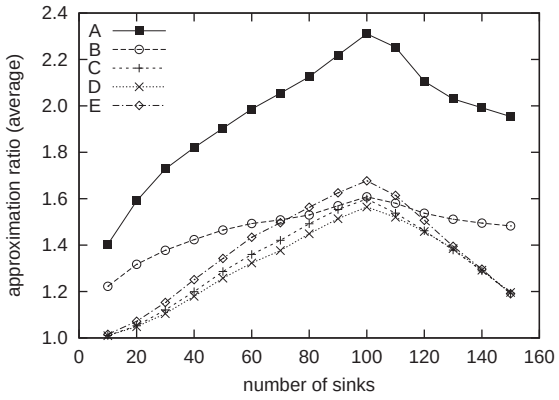


図 2.1: シンク数の変化

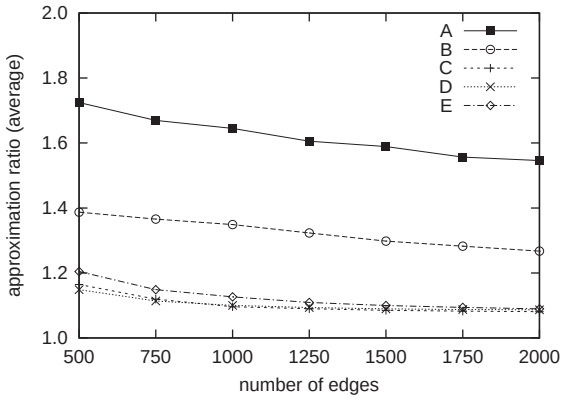


図 2.3: 辺数の変化

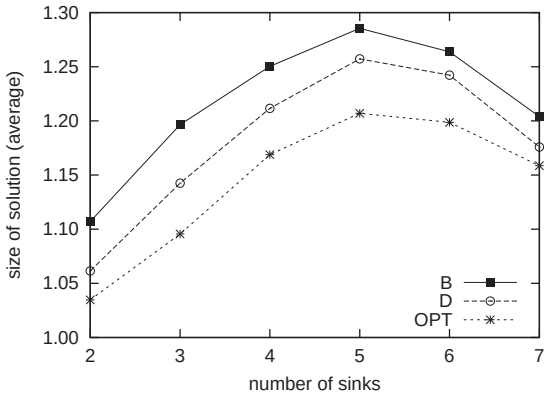


図 2.2: 最適解との比較

ので，提案手法の結果が非常に良くなった．辺数が増加すると，どの手法も得られる解が多少良くなるが，大きな変化はない．

需要を変化させた場合　こんどは，各点の需要をシンクまでの距離によって定めた．各点 v から最も近いシンクまでの距離 (ホップ数) を $h(v)$ とする．このとき，各点の需要を $h(v)+1$ とした場合 (以下**昇順**) と，$1/(h(v)+1)$ とした場合 (以下**降順**) について，一様乱数との比較を行った．表 2.1 は，それぞれの需要の与え方と手法に対して，点数 200，辺数 1,000，シンク数 50 の 1,000 個のインスタンスにおける近似率の分布である．

手法 A, B は昇順に対してはあまり変化せず，降順の場合には一様乱数の場合より良い結果となった．Chen et al. の手法は，シンクに隣接した点 (境界点) からフローを決定するため，シンクに近い点の需要が大きい降順で良い結果が得られたと考えられる．

手法 C は，一様乱数と比べて昇順，降順ともに悪くなり，特に昇順の結果が悪くなった．C の初期解である A は，降順において一様乱数より良い結果となったが，C の解は悪くなったことから，提案手法の性能は必ずしも初期解の良さに依存するわけではないといえる．

手法 D は，昇順に対してやや悪くなり，降順に対しては一様乱数よりも良い結果になった．悪い結果になった昇順の場合でも，すべての手法の中では最も良い結果になっている．

手法 E は，一様乱数の場合には A, B よりも良い結果になったが，需要を昇順，降順とした場合には，非常に悪い結果になった．昇順では，近似率 4 を超える場合もあった．手法 E の反復回数は，需要を一様乱数で与えた場合には平均 57.8 回だったのに対して，昇順の場合には 3.1 回であり，初期解からの改善がほとんど行われていない (表 2.3)．

初期解に対する提案手法の解の変化　さらに，初期解に対する提案手法の解の分布を求めた．表 2.2 は，点数 200，辺数 1,000，シンク数 50，需要を一様乱数で与えたときの，初期解 (手法 B により得られる解) と提案手法の解 (手法 D により得られる解) の関係を表したものである．この例では，B の解の大きさによらず，D の解が $[1.2, 1.3)$ となったものが多かった．また，B の解が悪かったにもかかわらず D の解が良くなったもの (表の左下) や，B の解をほとんど改善できなかったもの (表の右側) もあった．

しかし，需要を昇順，降順としたときに手法 E

の解が悪くなったように，提案手法は悪い初期解を与えた場合に必ずしも大きく改善できるわけではない．

計算時間と反復回数　最後に，計算時間と提案手法の反復回数について述べる．手法 C, D, E の計算時間には，初期解を求める時間も含まれる．いくつかの結果を表 2.3 に示す．

提案手法の計算時間は反復回数に依存する．需要を昇順，降順で与えた場合には，一様乱数の場合に比べて，どの手法も反復回数が大きく減少している．これは，一様乱数に比べて局所解が多くなり，すぐに反復が停止してしまうためだと考えられる．また，辺数が多くなると提案手法の反復回数は増加する．

インスタンスが大きくなると，反復回数の少ない手法 D の計算時間が提案手法の中では最も短くなる．手法 D は，5,000 点のインスタンスに対して 3 分程度で解が求まっており，これは実用時間内であるといえる．

考察

本節では，Chen et al. の手法と提案手法に対して実験的性能評価を行った．Chen et al. の手法は，理論的に証明されている近似保証よりも良い結果になった．

シンク数が点数の 1/2 のときにはどの手法も悪い結果となったが，これは合流フローの最適解と，下界として用いている分割可能フローとのギャップが大きくなるためだと考えられる．

どのような入力に対しても，提案手法である手法 D の解が最も良くなった．点数 5,000，辺数 50,000，シンク数 500，需要を一様乱数で与えた場合 (表 2.3 の 8)，手法 B の近似率の平均が 1.425 だったのに対して，手法 D では 1.065 に改善された．大きなインスタンスに対して，手法 D は提案手法の中で最も短い計算時間で解が求まり，従来手法と比較しても大きな増加にはなっていない．

初期解に近似保証が与えられていない手法 E は，需要が一様乱数の場合には良い結果が得られるが，昇順，降順とした場合には非常に悪い結果となるので，有用ではないといえる．

2.5　結論

本論文では，合流フローの混雑最小化問題に対する近似アルゴリズムの実験的性能評価を行った．本論文で提案した貪欲改善法は Chen et al. の手法 [1] に比べて，実際的性能が大きく向上した．

今後の課題としては，以下のことが挙げられる．

- 近似率・計算時間に関して，提案手法の理論的解析を行う．
- 新たな手法を提案する．
- モデルを拡張する (シンクの処理能力が異なる場合や多品種の問題など)．

参考文献

[1] J. Chen, R. D. Kleinberg, L. Lovasz, R. Rajaraman, R. Sundaram and A. Vetta: “(Almost) Tight Bounds and Existence Theorems for Confluent Flows”, *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*, Chicago, Illinois, pp. 529–538, June 2004.

[2] J. Chen, R. Rajaraman and R. Sundaram: “Meet and Merge: Approximation Algorithms for Confluent Flows”, *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, San Diego, California, pp. 373–382, June 2003.

[3] Y. Dinitz, N. Garg and M. Goemans: “On the Single-Source Unsplittable Flow Problem”, *Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science*, Palo Alto, California, pp. 290–299, November 1998.

[4] J. Kleinberg: “Single-Source Unsplittable Flow”, *Proceedings of the 37th Annual IEEE Symposium on Foundations of Computer Science*, Burlington, Vermont, pp. 68–77, October 1996.

[5] J. Kleinberg, Y. Rabani and E. Tardos: Fairness in Routing and Load Balancing. *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science*, New York City, pp. 568–578, New York, October 1999.

[6] 小島政和・土谷隆・水野真治・矢部博：“内点法”，朝倉書店，東京，2001.

[7] 田村明久・村松正和：“工系数学講座 17 最適化法”，共立出版，東京，2002.

表 2.1: 需要の変化

	一様乱数					昇順					降順				
近似率	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E
[1.0, 1.2)	0	0	96	205	24	0	0	0	5	0	0	22	0	227	0
[1.2, 1.4)	0	294	819	754	747	0	370	18	811	0	20	674	388	757	0
[1.4, 1.6)	35	597	79	40	207	53	524	392	170	0	355	291	523	16	20
[1.6, 1.8)	312	102	6	1	22	257	93	437	13	2	404	12	77	0	261
[1.8, 2.0)	379	7	0	0	0	441	13	130	1	26	178	1	12	0	344
[2.0, 2.2)	184	0	0	0	0	161	0	19	0	146	38	0	0	0	250
[2.2, 2.4)	67	0	0	0	0	70	0	4	0	250	4	0	0	0	102
[2.4, 2.6)	21	0	0	0	0	13	0	0	0	213	1	0	0	0	16
[2.6, 2.8)	1	0	0	0	0	5	0	0	0	188	0	0	0	0	5
[2.8, 3.0)	0	0	0	0	0	0	0	0	0	92	0	0	0	0	2
[3.0, 3.2)	1	0	0	0	0	0	0	0	0	42	0	0	0	0	0
[3.2, 3.4)	0	0	0	0	0	0	0	0	0	21	0	0	0	0	0
[3.4, 3.6)	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0
[3.6, 3.8)	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0
[3.8, 4.0)	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0
[4.0, 4.2)	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0

表 2.2: 初期解と提案手法の解の関係

初期解	提案手法の解 (D の解)							
(B の解)	[1.1, 1.2)	[1.2, 1.3)	[1.3, 1.4)	[1.4, 1.5)	[1.5, 1.6)	[1.6, 1.7)	[1.7, 1.8)	計
[1.2, 1.3)	9	27	0	0	0	0	0	36
[1.3, 1.4)	63	151	44	0	0	0	0	258
[1.4, 1.5)	77	224	77	18	0	0	0	396
[1.5, 1.6)	41	116	35	5	4	0	0	201
[1.6, 1.7)	14	42	20	7	1	0	0	84
[1.7, 1.8)	1	10	3	3	0	0	1	18
[1.8, 1.9)	0	1	2	0	2	0	0	5
[1.9, 2.0)	0	1	1	0	0	0	0	2
計	205	572	182	33	7	0	1	1,000

表 2.3: 計算時間と反復回数

	インスタンス				A	B	C		D		E	
	n	m	k	需要	時間	時間	時間	反復	時間	反復	時間	反復
1	200	1,000	50	昇順	0.1017	0.2186	0.1130	1.75	0.2330	2.30	0.0115	3.14
2	200	1,000	50	降順	0.0961	0.2150	0.1068	2.04	0.2260	1.21	0.0114	3.59
3	200	1,000	50	乱数	0.0988	0.2279	0.1572	18.51	0.2492	5.67	0.1346	57.84
4	200	1,000	100	乱数	0.1441	0.4933	0.2087	15.79	0.5006	1.04	0.1718	60.97
5	200	2,000	50	乱数	0.1144	0.2421	0.3289	28.46	0.3355	10.12	0.5061	93.44
6	500	5,000	50	乱数	0.4182	0.5990	2.0120	75.10	1.6599	49.32	3.3198	203.6
7	1000	10,000	100	乱数	1.7189	2.2631	8.0462	138.2	6.3063	84.23	17.469	445.1
8	5000	50,000	500	乱数	78.564	73.333	286.20	574.3	187.95	307.3	646.03	2241

計算時間，反復回数ともに平均値である．また，計算時間の単位は秒である．

研究業績一覧

著書

1. 浅野孝夫，平田富夫，小野孝男，浅野泰仁: “組合せ最適化（B. Korte and J. Vygen: Combinatorial Optimization: Theory and Algorithm, Springer, 2002 の日本語訳）”, シュプリンガー・フェアラーク東京, （2005 年 7 月刊行予定）.
概要: 組合せ最適化の全般を簡潔にまとめた本で最新の成果まで含む内容である (参考文献には 2005 年出版のものもある)。全部で 21 章からなり、その詳細は以下の通りである。第 1 章 はじめに、第 2 章 グラフ、第 3 章 線形計画法、第 4 章 線形計画アルゴリズム、第 5 章 整数計画法、第 6 章 全点木と有向木、第 7 章 最短パス、第 8 章 ネットワークフロー、第 9 章 最小費用フロー、第 10 章 最大マッチング、第 11 章 重み付きマッチング、第 12 章 b-マッチングと T-ジョイン、第 13 章 マトロイド、 第 14 章 マトロイドの一般化、第 15 章 NP-完全性、第 16 章 近似アルゴリズム、第 17 章 ナップサック問題、第 18 章 ビンパッキング問題、第 19 章 多品種フローと辺素パス、第 20 章ネットワーク設計問題、第 21 章 巡回セールスマン問題。

学術論文

1. Takao Asano:
“An Improvement of Yannakakis’ Algorithm for MAX SAT”, Journal of the Institute of Sceince and Engineering, Chuo University, 9, pp.57 – 77, 2004.
概要: MAX SAT (maximum satisfiability problem) is stated as follows: given a set of clauses with weights, find a truth assignment that maximizes the sum of the weights of the satisfied clauses. In this paper, we consider approximation algorithms for MAX SAT proposed by Yannakakis and Goemans-Williamson and present an approximation algorithm which is an improvement of Yannakakis’ algorithm. Although Yannakakis’ original algorithm has no better performance guarantee than Goemans-Williamson, our improved algorithm has a better performance guarantee and leads to a 0.770-approximation algorithm.

2. 浅野孝夫，九里史郎，上ヶ原誠:
“施設配置問題とスケジューリング問題に対する高性能近似アルゴリズムの実験的性能評価”, 中央大学理工学研究所論文集, 9, pp.79 – 97, 2004.

概要: NP-困難な問題に対して多項式時間で最適解を求めるのは困難であるので，最適解に近い近似解を多項式時間で求めて使用することが多い．$\alpha \geq 1$ に対して，最小化問題ならば，いつも最適解の α 倍以下の解を入力サイズの多項式時間で求めるようなアルゴリズムを α-近似アルゴリズムという．最小化問題に対する α を近似率あるいは精度保証という．一方，実時間処理アルゴリズムでは，入力情報が得られた時点で，それ以降の情報がくる前に処理を実行 (確定) することが要求される．入力の情報がすべて得られてから処理を実行する通常のアルゴリズムに対して，このようなアルゴリズムはオンラインアルゴリズムと呼ばれる．最小化問題に対して，オンラインアルゴリズムによって得られる目的関数値が (オフライン環境における) 最適な目的関数値の ρ 倍以下であるとき，ρ を競合比という．精度保証付きの近似アルゴリズムやオンラインアルゴリズムの競合比の研究は近年精力的に実行され，様々なアルゴリズムが提案されてきている．本論文では，そのようなアルゴリズムから，施設配置問題とスケジューリング問題に対して理論面から最近提案された代表的アルゴリズムを選び，それらを実装して，その実際的性能評価を与える．さらに，実際の状況に適したヒューリスティクスを提案し，その有効性も検証する．

研究会等

1. 二瓶浩一，浅野孝夫:
   “合流フローの混雑最小化アルゴリズムに対する実験的性能評価と貪欲改善”, 情報処理学会アルゴリズム研究会報告, AL98-7, pp.41–48, 2004.
   概要: ネットワーク・フローの中で,「すべての点においてフローが出て行く辺が 1 本以下」という条件を満たすものを合流フローという．インターネット・ルーティングをはじめとして，現実社会において合流フローとなる例は数多く存在する．入力として，有向グラフ・複数のシンク・各点の需要が与えられたとき，すべての点の需要をシンクに流す合流フローの中で混雑が最小になるものを求める問題を，合流フローの混雑最小化問題という．本論文では，この問題に対して 2004 年に Chen et al. によって提案された手法の実験的性能評価を行い，得られた解に貪欲改善を加えると性能が大きく向上することを示す.

2. 佐々木 浩高，浅野孝夫:
   “Reverse-Fit を用いた単純な 2 次元ビンパッキングのアルゴリズム”, 情報処理学会アルゴリズム研究会報告, AL93-16, pp.113–120, 2004.
   概要: 高さと幅が 1 以下の長方形を辺の長さが 1 の単位正方形に重ならないようにパッキングするとき, 必要な正方形の個数を最小にするという問題が 2 次元ビンパッキング問題である．この問題に対して, 2002 年に発表された Caprara のアルゴリズムは漸近近似率が良くなるように作られたものであり, 現実的な入力においては多くの場合良い結果とならない．本論文では現実的な入力において良い結果を出せるようなアルゴリズムを提案し, 計算機上に実装して実験的性能の比較評価を行う.

学会大会等

1. 浅野孝夫:
   “近似アルゴリズムの近似性能の改善とその限界 (特別講演)”, 日本数学会 2004 年度年会応用数学分科会講演アブストラクト, pp.46 – 65, 2005 年 3 月.

2. 中塩英良，浅野孝夫:
   “施設配置問題に対する近似アルゴリズムの実験評価”, 日本オペレーションズ・リサーチ学会２００４年度秋季研究発表会アブストラクト集, pp.64 – 65, 2004 年 9 月.

C04: 実践的な列挙アルゴリズムの理論構築

宇野 毅明 † 中野 眞一 ‡

† 国立情報学研究所情報学基礎研究系
〒 101-8430 東京都千代田区一ツ橋
uno@nii.jp

‡ 群馬大学工学部情報工学科
〒 376-8515 群馬県桐生市
nakano@cs.gunma-u.ac.jp

2004 年度は，列挙アルゴリズムの研究にとって発展の年であった．最適化，人口知能，データベースなどの情報学分野を中心に列挙を用いたモデル化が行われ，物理・化学をはじめとする他の科学領域，および産業分野でも，それらのモデルを用いた研究が進められている．特に機械学習やデータマイニングといった，数理的な対象を分析し，知識を発見する分野において，列挙アルゴリズムが広く使われ，また研究されてきている．応用分野においても，web データ，テキストデータ，実験データ，金融時系列データ，顧客データ，販売データ，事故・故障記録データ，ゲノム配列など，機械的に収集された巨大なデータがますます増加し，そこから有用な情報を探し出すためには，列挙のような網羅的なアプローチを高速に行うことが肝要となっている．このため，ここ 1-2 年で列挙を用いたモデル化とその解法は活発に研究されてきたが，複雑な構造の列挙は容易でないため，簡単な構造、あるいはその列挙手法に工夫を加えて構築したモデル・解法の研究が多くなっている．

また，巨大データの取り扱いのため，列挙アルゴリズムの高速化に対しては，以前よりも要求が高まってきている．高速な列挙アルゴリズムの開発のみに焦点をあてた研究も増えてきており，特に著名な問題においては，多くの研究が行われている．しかし，これらの研究はそれほど系統立てて行われているわけではなく，いくつもの技術が乱立している．この問題点を解決しようと，データマイニング分野において，データベース中に頻出する集合を列挙する問題に対するプログラムのコンテストが 2003 年度，2004 年度と 2 回にわたって行われてきた．このコンテストには多くのアルゴリズムとその実装が投稿され，応用分野から取り出したデータセットに対して，計算効率の検証が行われた．結果，多くの技術が 1 箇所に集積され，参照されることとなり，頻出パターン列挙に関する応用研究の大きな助けとなっている．また，このコンテスト以降，頻出する集合の列挙アルゴリズムの開発研究は多少減少したようだが，これは技術の整理によって，無駄な開発が行われなくなったと見るべきであろう．本研究課題からも，このコンテストにプログラムの投稿を行った．このプログラムは，審査の結果，最優秀賞を収めることができた．これは，理論的なアルゴリズム研究に対して，実践的な技術を付加し，応用上有用なアルゴリズムの設計理論を構築しようとする，本研究課題の方向性が世界的な舞台でも認められ，その有効性が実証されたと言えるであろう．

これら世界的な情勢を踏まえ，本研究課題では，今年度の研究の焦点を，データマイニングなどで頻繁に用いられるグラフのクリークを列挙するアルゴリズムの高速化と，幾何学的な構造の列挙アルゴリズムの開発にあてた．グラフのクリークとは，そのグラフの頂点の部分集合で，全ての頂点間に枝が存在するもののことをいう．クリークは，グラフ中の局所的に密な部分に対応する構造であるため，さまざまなモデル化に用いられている．例えば，グラフの頂点集合がある種のものの集合になっており（つまりは，各頂点が各ものと 1 対 1 の対応をする），関係のあるものとものの間に枝があるようなグラフにおいては，クリークはお互いに関係あるものの集合となる．このため，クリークはクラスタリング，ルール発見，分類など多くの情報的アプローチにおいてモデル化に使われており，非常に重要な構造である．

グラフの頂点集合が A と B に分割され，グラフの任意の枝が A と B の頂点を結んでいる場合，そのグラフは 2 部グラフであるという．2 部グラフは，2 つの種類のデータの対応を表すため，多くの構造が 2 部グラフとして表現される．例えば

行列や，項目の集合，論理式も 2 部グラフで表現される．2 部グラフの頂点集合 S が，S の A に含まれる頂点と B に含まれる頂点の任意の組に対して，その間に枝が存在するとき，S は 2 部クリークと呼ばれる．2 部クリークも，クリークと同様，2 部グラフ上の特徴的な集合，局所的に密な構造を表す構造である．

グラフのクリークを列挙する問題は，計算量的にはさほど難しくない．クリーク 1 つあたり，グラフの頂点数に比例する時間で見つけることができ，とくに疎なグラフにおいては，実験的に，1 つあたりほぼ定数時間で見つけられることが確認されている．列挙手法も単純であり，プログラミング，つまり実装も容易である．しかし，極大なクリーク，つまり他のクリークに含まれないようなクリークのみを見つけようとすると，さほど自明な問題ではなくなる．

応用上，極大なクリークの発見は重要である．クラスタリングや知識発見など，多くの応用では，候補となる解数の本質的な減少が大きな課題である．その上，数の減少に伴う情報の損失を極力避けなければならない．こういった意味では，極大なクリークのみを列挙するという手法は，任意のクリークは少なくとも 1 つの極大クリークに含まれ，かつこれらのクリークは極大クリークの部分集合として容易に生成できることから情報の損失がなく，また極大クリークの数は一般的にクリークの数より小さく，場合によっては指数的に小さいため，極めて有効である．

極大クリークの列挙アルゴリズムは，古くから研究が行われている．1978 年に築山らによって，極大クリーク 1 つあたりグラフの枝数と頂点数の積に比例する時間しかかからない，多項式時間アルゴリズムが提案されている．この後 30 年近く，計算量的な改善は行われてこず，計算量の改善が可能かどうかは列挙アルゴリズムの大きな未解決問題であった．

本年度の研究では，この極大クリーク列挙問題に対して，理論的な計算量の改善が可能であるかを検討し，新たなアルゴリズムの開発を目指した．その結果，アルゴリズムの各反復を行列積の計算に類似した処理で行うことにより，行列積で行われてきた計算量改善の結果を極大クリークの列挙に応用することに成功した．この結果，極大クリーク列挙の，極大クリーク 1 つあたりの計算量は，行数がグラフの頂点数に比例する正方行列の掛け算の計算量と等しくなった．この結果，ある程度密なグラフにおいては，既存のアルゴリズムよりも計算量の意味で改善が行われることとなった．

また，疎なグラフに対する極大クリーク列挙アルゴリズムの計算量の改善についても研究を行った．この研究では，上記のアルゴリズムとは異なり，グラフの疎性を上手に利用したアルゴリズムの開発を中心に行った．その結果，極大クリーク 1 つあたりの計算量を，グラフの最大次数の 4 乗で抑えることに成功した．この結果は，グラフの最大次数が大きく，特に頂点数に比例する場合などは，計算量的な改善はないが，入力したグラフが疎であり，最大次数が小さい場合には計算量の改善を導く．また，計算実験の結果，ある程度ランダムなグラフや，実データのグラフにおける実験的な計算時間はグラフの平均次数にほぼ比例することがわかった．これは，出力の大きさに計算時間がほぼ比例するということを示しており，近年研究されている疎なデータに対する分析や知識発見への応用としては，十分な結果といえるだろう．

また，この研究を発展させ，2 部グラフの極大 2 部クリークを高速に列挙するアルゴリズムの開発も行った．2 部グラフの極大 2 部クリークは，グラフに変換処理を行うことで，元のグラフの極大 2 部クリークが新しいグラフの極大クリークとなるようにすることができ，また逆も成り立つ (新しいグラフの極大クリークが元のグラフの極大 2 部クリークとなる)．よって，入力した 2 部グラフを変換して，極大クリークを列挙することにより，全ての極大 2 部クリークを列挙することができる．よって，計算量的には，極大 2 部クリークの列挙は容易に解ける問題である．しかし，この変換は，グラフに多量の枝を付加するため，疎なグラフを密なグラフに変換してしまう．そのため，上記の疎なグラフに対して有効なアルゴリズムを用いても，疎な 2 部グラフの極大 2 部クリークの列挙は効率良く行えない．そこで，このような変換を行うことなく極大 2 部クリークの列挙を行うため，極大クリーク列挙アルゴリズムの改良を行った．極大 2 部クリークは極大クリークにない良い特徴づけを持つため，結果として極大クリークの列挙よりも小さい計算量のアルゴリズムを開発するこ

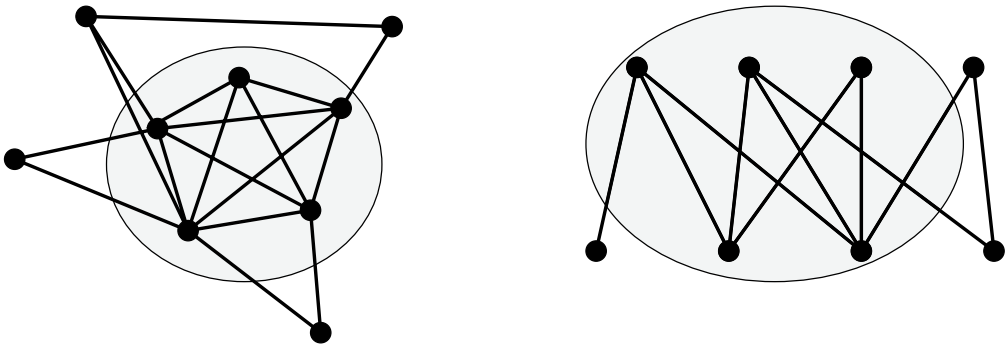


図 2.1: グラフの極大クリークと，2 部グラフの極大 2 部クリーク

とに成功した．極大 2 部クリーク 1 つあたりの計算量は最大次数の 3 乗となった．また，計算機実験によって，実データおよびランダムなグラフにおける計算時間は，極大クリーク列挙時のそれよりも 10 倍程度短くなっていることを確認した．

極大 2 部クリークは様々な場面において応用があり，特にデータマイニングでは重要な位置を占めるため，多くの研究が行われている．データマイニングの基礎的な問題の 1 つに，頻出集合列挙問題がある．各項目がアイテムの集合となっているようなデータベースをトランザクションデータベースという．トランザクションデータベースは，商品売り上げデータ，アンケートデータ，辞書データ，グラフデータなど，多くのデータを取り扱える基礎的な構造である．

トランザクションデータベースのある定数個以上の項目に含まれるようなアイテムの集合を頻出集合とよぶ．また，定数をサポートとよぶ．頻出集合はそれ自体が知識を発見するためのモデルとなるばかりでなく，データベースを分析する際の特徴の 1 つとなる．そのため，与えられたデータベースとサポートに対して，頻出集合を全て見つけるという問題は，データマイニングの分野でも非常に基礎的な問題であり，多くの研究と，アルゴリズムの実装が存在する．

サポートが小さくなるにつれ，頻出集合の数は指数的に大きくなる．興味深い集合を発見し損こなうことがないようにするためには，サポートの値を小さく設定する必要があるのだが，その結果非常に多くの頻出集合を見つける必要が発生する．このため，意味的な情報を失わずに，頻出集合の集合から代表を選びだし，それのみを列挙するモデルが考案されている．1 つは極大頻出集合であり，もう 1 つは頻出飽和集合である．極大頻出集合は他の頻出集合に真に含まれないような頻出集合のことであり，飽和集合とは，頻出度が等しい，つまり同数のトランザクションに含まれるような他の頻出集合に真に含まれないような集合のことである．

トランザクションデータベースを 2 部グラフとみなすと，飽和集合と極大 2 部クリークが 1 対 1 に対応することが知られている．そのため，極大 2 部クリークの列挙アルゴリズムを頻出度順に出力するよう改良することにより，頻出飽和集合列挙アルゴリズムを得ることができる．しかし，既存の極大 2 部クリーク列挙アルゴリズムは疎で巨大なデータを取り扱うことができなかったため，頻出飽和集合列挙に理論的なアルゴリズムを適用することはできなかった．そのため，既存の頻出飽和集合列挙アルゴリズムは，ヒューリスティックな枝狩りを中心とした実用的な側面のみに注目したいた．本研究課題の研究により，理論的なアプローチに基き，かつ疎で巨大なデータも扱えるようなアルゴリズムが誕生することとなった．

データマイニング分野では，実装の有効性に関する議論にも重きが置かれている．そのため，頻出集合列挙問題においても，単なる手法の理論の研究にとどまらず，実際のデータに対してどの程

データベース	
1,2,5,6,7,9	**3つ以上の項目に**
2,3,4,5	**含まれるアイテム集合**
1,2,7,8,9	{1} ***{2}*** {7} {9}
1,7,9	{1,7} {1,9}
2,7,9	{2,7} {2,9} ***{7,9}***
2	***{1,7,9} {2,7,9}***

図 2.2: トランザクションデータベースと，サポートが 3 である場合の頻出集合，太字は頻出飽和集合

度有効な実装が行えるかという点についても研究が進められている．昨年度，今年度と実装の有効性に関するコンテストが行われた．世界の研究者がプログラムを投稿し，それぞれの有効性を計算実験により検証するというものである．15 種類程度の実際のデータから得たトランザクションデータベースそれぞれに対し，いくつかのサポートに対する計算時間を計測することで比較が行われた．

我々も，極大 2 部クリーク列挙アルゴリズムに実装上の工夫を追加したプログラムを作成し，投稿した．我々のプログラムは，理論的に裏づけされた列挙手法を用いているため，他のプログラムに比べて計算の無駄が少なく，また，メモリの使用量も少ない．計算実験による検証の結果，我々のプログラムは 6 割以上の例題で一番の成績を収め，結果最優秀賞を受賞した．

このコンテストでは，頻出飽和集合列挙プログラムの他，頻出集合・極大頻出集合の列挙に関するプログラムのコンテストも合わせて行われた．両者ともに，頻出飽和集合の列挙手法を用いると，効率的に列挙できる．今回我々は，この列挙手法をベースに実装上の工夫を加えたプログラムを開発し，投稿した．計算実験の結果，これらのプログラムも優秀な成績を収めた．

今年度は，クリーク列挙以外の，データマイニングへの応用を意識した研究も行っている．グラフ構造を持つデータを分析するグラフマイニングの分野では，グラフの中に頻出するパターンを見つける研究が盛んに行われている．パターンとしては，例えばパスや木，サイクル，部分グラフなどが研究されている．

頻出集合列挙とは異なり，グラフの頻出パターン列挙には計算的な困難が発生する．集合の場合，異なる 2 つのパターンが等しいことは簡単に確認できるが，グラフの場合，2 つのパターンが等しいことを判定する作業はグラフが同型であるかどうかを判定する問題を含むため，計算量的に困難である．このため，グラフパターンの効率的な列挙が難しく，メモリの意味でも計算時間の意味でも，効率的なアルゴリズム，および高速なプログラムを作ることは難しい．

現在までに行われている研究は，同型性の判定，および列挙が効率的に行えるようなグラフクラスに属するパターンのみに対象を限定した列挙問題が研究されている．例えば，パスやサイクルは同型性の判定が自明であるし，木も線形時間で同型性の判定が可能である．パスやサイクルであるパターン，つまり長さが n であるようなパスやサイクルの列挙は容易であるが，木の列挙はそれほど自明ではない．既発見解をメモリに蓄えずに重複を避けるような，メモリ効率と計算効率の良いアルゴリズムを構築するためには，全ての木を効率良くたどれるような探索ルートを用いた列挙手法が必要である．単純な方法で探索ルートを生成すると，重複や見つけ損ないを回避できない．

このような，単純な手法での列挙が難しい構造を列挙する際に威力を発揮するのが逆探索である．逆探索は，列挙しようとしている構造の間に非閉路的な親子関係を定める．非閉路的な親子関係は木型の探索ルートを導出するため，この探索ルートをたどることで，全ての列挙対象を発見するという手法である．列挙を行う際には，根となる木を出発し，親から子への移動を繰り返すことにより，深さ優先的に探索を行う．この際，現在訪れ

ている解の子供を効率良く発見できるようにするため，親子関係の定義を工夫することと，アルゴリズムの開発が重要となる．

今年度の我々の研究では，逆探索を利用して木を効率良く列挙するアルゴリズムの開発を行った．木を根付き木とみなすと，根の位置の変更や子供の順番の変更で１つの木から様々な根付き木が生成される．そこでまず，木に対して唯一的に定まるような根の定め方を定義し，子供の順番もグラフの構造のみに依存して唯一的に定まるような定め方を定義した．この方法で定義した根と子供の順番は木に対する唯一的な標準型を与える．標準型の形状は唯一的に定まっているため，通常の木よりも取り扱いが簡単となる．次に，標準型と標準型の間に親子関係を定めることで，木の間に親子関係を定めた．

この親子関係では，親に１つ頂点を追加することによって子供が得られ，また，子供を生成するような，頂点の追加場所は，木の右端部分に連続して存在する．そのため，子供を１つあたり定数時間で生成することができ，全体として木を１つあたり定数時間で列挙するようなアルゴリズムを導くこととなった．

データマイニングの問題では，データベースの木の各頂点にはラベルが付加されていることが多い．そのような場合，見つけ出すパターンとしては，ラベルがついた木が要求されている．今年度の研究では，このようなラベル付きの木を列挙するためのアルゴリズムも開発した．単にラベルが付いた木を列挙するのであれば，木を列挙した後，それにラベルを付ければよい．しかし，頻出するパターンを見つける場合には，このような列挙手法を用いると効率が悪くなる．ラベル付きの木を直接，小さいものから大きいものへと成長させるような手法で生成する必要がある．今年度の研究で開発したアルゴリズムは，このような列挙手法に基づいて構築されており，頻出するパターンの発見に応用した場合に効率良いアルゴリズムを導ける．また，このアルゴリズムの計算時間は１つあたり定数時間であり，効率が良い．

近年は様々な場面で列挙アルゴリズムが使われるようになり，そのため，様々な構造に対する効率の良い列挙法が求められている．簡単な構造であれば，効率良い列挙法の構築は容易なのだが，複雑で取り扱いの難しい構造となると，計算効率を考えずに単純に構築された列挙法に基づくアルゴリズムは，ときに効率の良いアルゴリズムに比べて何千倍も余計に計算時間を費やすこともある．特に，幾何的な構造は列挙が難しいことが多い．そのため，今年度は幾何学的な構造に対する効率的な列挙手法の研究も行った．以下にそれらの概要を示す．

まず研究を行ったのが，根付き三角形分割の列挙手法である．与えられた平面上の点集合に対して，その点同士を結んで平面の分割を平面分割とよぶ．特に全ての面が三角形であるとき，三角形分割とよぶ．三角形分割の一本の枝が根として指定されたとき，それを根付き三角形分割とよぶ．三角形分割はグラフ描画や数値計算に多数の応用がある重要な幾何構造である．本年度は，n 個以下の点から作られる三角形分割を，同型であり，かつ根が等しいような三角形分割を同一視して列挙する問題を研究した．

三角形分割の同型性判定はそれほど困難ではないが，重複を効率良く避けて列挙を行うことはそれほど容易ではない．単純な手法ではすぐに重複が発生するか，あるいは見つけ損いがでてしまう．そこで，三角形分割の間を移動する関係を定め，三角形分割の上に探索木を定義した．この結果，効率良く全ての解を探索できるようになり，根付き三角形分割１つあたり定数時間しかかからないようなアルゴリズムを構築することに成功した．

また，このアルゴリズムを拡張することにより，ちょうど n 個の点からなる三角形分割 (根付きではないことに注意) を１つあたり $O(n)$ 時間で列挙するアルゴリズムを得た．このアルゴリズムは，外周上の点数がちょうど r 個である三角形分割の列挙も可能であり，この場合の計算時間は出力される三角形分割１つあたり $\mathrm{O}(r)$ 時間である．これらのアルゴリズムのメモリ使用量は $\mathrm{O}(n)$ であり，メモリ使用量の意味で最適である．

点の個数が n 個であり，面の個数が f 個であるような，異なる３次元多面体の個数を求めることは，幾何学における有名な未解決問題の１つである．また多面体の効率的な数え上げアルゴリズムもこれまで知られていなかった．全ての面が三角形であるような３次元の多面体は，平面の三角形分割に対応するため，上記の三角分割列挙アルゴ

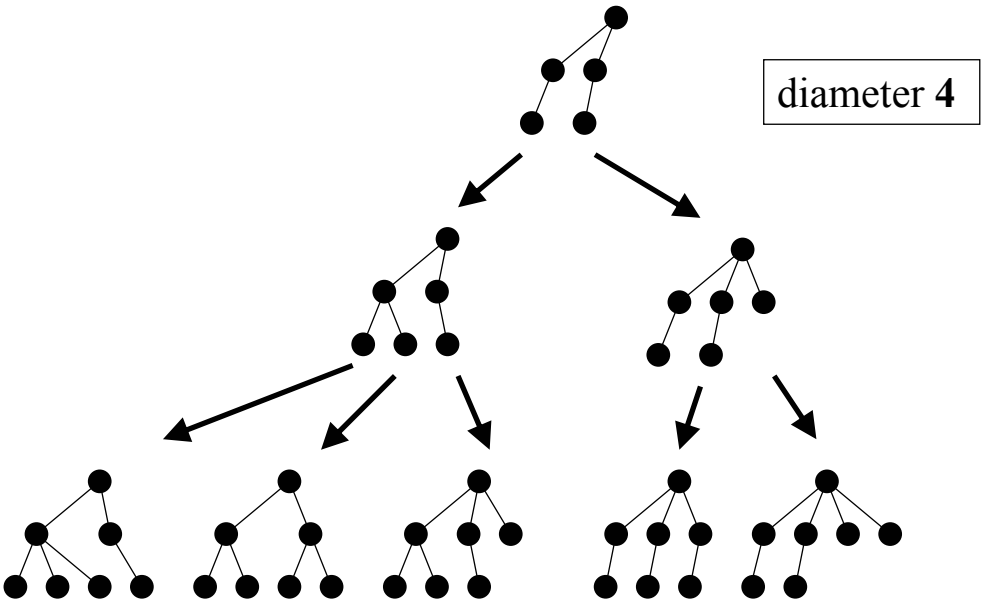


図 2.3: 直径が 4 で頂点数が 7 以下である木の集合上に定義された探索ルート

リズムを用いると，各面が三角形であるような 3 次元の多面体の列挙が行える．このアイディアに基づき，今年度の研究では効率的なアルゴリズムを開発した．さらに，このアルゴリズムの実装を行い，$4 \leq n \leq 15$ なる各 n について，点の個数が n であり全ての面が三角形であるような多面体の個数を数え上げた．また列挙した多面体の全てをグラフの形でデータベース化し，WWW 上のホームページにて公開している．

平面の三角形分割はリアライザと呼ばれる，ある特徴を持った内辺の分割を持つ．リアライザは平面グラフの描画アルゴリズム等に応用がある．与えられたグラフのリアライザの列挙は，自明でなく，既存の研究は存在しない．今年度の研究では, 左優先順序という極大平面グラフの点の順序づけを定義し, 左優先順序とリアライザ間の 1 対 1 関係を導くことにより，リアライザの標準形を定義した．さらに，標準形の集合上に効率良くたどれる探索木を定義することで，高速にリアライザを列挙するアルゴリズムを与えた．このアルゴリズムは, n 点からなる極大平面グラフのリアライザを, リアライザ 1 つあたり $O(n)$ 時間で列挙する．

グラフを, 各面が L 字形 (退化した L 字形として長方形を含む) であるように, かつ, 辺が交差することなく, 平面に描画したものを, グラフの L 字形描画とよぶ．L 字形描画はグラフをある種の規則にしたがって平面に描画したものである．グラフ描画の応用の観点からは，L 字描画のような基礎的な構造を列挙して最善の描画を選ぶような手法は基礎的な事項である．このような応用を鑑み，本年度の研究では, 全ての底辺付き L 字形描画を, 重複も抜けもなく列挙する高速なアルゴリズムの開発を行った．ただし，底辺付き L 字描画とは，L 字描画の外周上の辺の 1 つが底辺として指定されたものであり，ここでの列挙問題では，平面描画として同型であり，かつ底辺が等しいものは同一視している．本研究のアルゴリズムは, 内面の個数がちょうど n 個である底辺つき L 字形描画の全てを, 1 つあたり $O(1)$ 時間で生成する．また，メモリ使用量に関しても $O(n)$ であり，最適である．

研究業績一覧

学術論文

1. Takeaki Uno, Masashi Kiyomi, Hiroaki Arimura:
"LCM ver.2: Efficient Mining Algorithms for Frequent/Closed/Maximal Itemsets", Proceedings of IEEE ICDM'04 Workshop FIMI'04, 2004年11月.
概要: For a transaction database, a frequent itemset is an itemset included in at least a specified number of transactions. A frequent itemset P is maximal if P is included in no other frequent itemset, and closed if P is included in no other itemset included in the exactly same transactions as P. The problems of finding these frequent itemsets are fundamental in data mining, and from the applications, fast implementations for solving the problems are needed. In this paper, we propose efficient algorithms LCM (Linear time Closed itemset Miner), LCMfreq and LCMmax for these problems. We show the efficiency of our algorithms by computational experiments compared with existing algorithms.

2. Shin-ichi Nakano, Takeaki Uno:
"Constant Time Generation of Trees with Specified Diameter", Lecture Notes in Computer Science, 3353, 33-45, 2004年5月.
概要: Many algorithms to generate all trees with n vertices without repetition are already known. The best algorithm runs in time proportional to the number of trees. However, the time needed to generate each tree may not be bounded by a constant, even though it is "on average". In this paper we give a simple algorithm to generate all trees with exactly n vertices and diameter d, without repetition. Our algorithm generates each tree in constant time. It also generates all trees so that each tree can be obtained from the preceding tree by at most three operations. Each operation consists of a deletion of a vertex and an addition of a vertex. By using the algorithm for each diameter $2, 3, \cdots, n-1$, we can generate all trees with n vertices.

3. Kazuhisa Makino, Takeaki Uno:
"New Algorithms for Enumerating All Maximal Cliques", Lecture Notes in Computer Science, 3111, 260-272, 2004年7月.
概要: In this paper, we consider the problems of generating all maximal (bipartite) cliques in a given (bipartite) graph $G = (V, E)$ with n vertices and m edges. We propose two algorithms for enumerating all maximal cliques. One runs with $O(M(n))$ time delay and in $O(n^2)$ space and the other runs with $O(\Delta^4)$ time delay and in $O(n+m)$ space, where Δ denotes the maximum degree of G, $M(n)$ denotes the time needed to multiply two $n \times n$ matrices, and the latter one requires $O(nm)$ time as a preprocessing. For a given bipartite graph G, we propose three algorithms for enumerating all maximal bipartite cliques. The first algorithm runs with $O(M(n))$ time delay and in $O(n^2)$ space, which immediately follows from the algorithm for the non-bipartite case. The second one runs with $O(\Delta^3)$ time delay and in $O(n+m)$ space, and the last one runs with $O(\Delta^2)$ time delay and in $O(n+m+N\Delta)$ space, where N denotes the number of all maximal bipartite cliques in G and both algorithms require $O(nm)$ time as a preprocessing. Our algorithms improve upon all the existing algorithms, when G is either dense or sparse. Furthermore, computational experiments show that our algorithms for sparse graphs have significantly good performance for graphs which are generated randomly and appear in real-world problems.

4. Shin-ichi Nakano:
"Efficient Generation of Triconnected Plane

Triangulations", Computational Geometry Theory and Applications, 27, 109-122, （掲載予定）.

概要: A "rooted" plane triangulation is a plane triangulation with one designated vertex on the outer face. A simple algorithm to generate all triconnected rooted plane triangulations with at most n vertices is presented. The algorithm uses $O(n)$ space and generates such triangulations in $O(1)$ time per triangulation without duplications. The algorithm does not output entire triangulations but the difference from the previous triangulation. By modifying the algorithm all triconnected rooted plane triangulations having exactly n vertices including exactly r vertices on the outer face in $O(r)$ time per triangulation can be generated without duplicates, while the previous best algorithm generates such triangulations in $O(n^2)$ time per triangulation. All triconnected (non-rooted) plane triangulations having exactly n vertices including exactly r vertices on the outer face can also be generated without duplicates in $O(r^2n)$ time per triangulation, and all maximal planar graphs can be generated in $O(n^3)$ time per graph.

5. 高木正博, 中野眞一:
"L 字形描画の列挙", 電子情報通信学会論文誌 DI, J87-D-I, 1-11, 2004 年.

概要: グラフを, 各面が L 字形 (退化した L 字形として長方形を含む) であるように, かつ, 辺が交差することなく, 平面に描画したものを, グラフの L 字形描画とよぶ. 本文は, 全ての底辺つき L 字形描画を, 重複も抜けもなく列挙する高速なアルゴリズムを与える. 本文のアルゴリズムは, 内面の個数がちょうど n 個である底辺つき L 字形描画の全てを, 重複も抜けもなく, 描画 1 つあたり $O(1)$ 時間で生成する. このアルゴリズムが使用する作業用記憶領域はアルゴリズム全体で $O(n)$ である.

6. H. Tanaka and S. Nakano:
"Efficient Generation of Plane Triangulations with Specified Maximum Degree", 電子情報通信学会英文論文誌 Special issue on Foundations of Computer Science, Vol.E87-D, 330-336, 2004 年.

概要: A "based" plane triangulation is a plane triangulation with one designated edge on the outer face. In this paper we give a simple algorithm to generate all biconnected based plane triangulations having exactly n vertices and with the maximum degree exactly D. The algorithm uses $O(n)$ space and generates such triangulations in $O(1)$ time per triangulation without duplications.

7. 佐藤広幸, 金子雄一, 中野眞一:
"多面体の数え上げ", 電子情報通信学会論文誌 A, J87-A, 1419-1424, 2004 年.

概要: 点の個数が n 個であり，面の個数が f 個であるような，異なる 3 次元多面体の個数を求めることは，幾何学における有名な未解決問題の 1 つである．また多面体の効率的な数え上げアルゴリズムもこれまで知られていなかった．最近, 底辺つき極大平面的グラフを，効率良く列挙するアルゴリズムが，我々によって設計された．本文では，このアルゴリズムを基にして, 全ての面が三角形であるような多面体の効率的な数え上げアルゴリズムを設計する．また，このアルゴリズムを実装し，$4 \leq n \leq 15$ なる各 n について，点の個数が n であり全ての面が三角形であるような多面体の個数を数え上げたので報告する．また列挙したグラフの全てを WWW 上で公開したので報告する．

8. 山中克久, 中野眞一:
"リアライザの列挙", 電子情報通信学会論文誌 DI, （掲載予定）.

概要: 極大平面グラフ (全ての面が三角形である平面グラフ) が与えられたとき, ある条件を満たすような内辺の分割をそのグラフのリアライザとよぶ. リアライザは平面グラフの描画アルゴリズム等に応用がある. グラフ G が与えられたとき, G のリアライザを列挙

するアルゴリズムは, これまで知られていなかった. 本文は, まず, 左優先順序という極大平面グラフの点の順序づけを定義し, そして, 左優先順序とリアライザには 1 対 1 の対応関係があることを示す. このことを利用して, リアライザを重複も抜けもなく高速に列挙するアルゴリズムを与える. 本文のアルゴリズムは, n 点からなる極大平面グラフのリアライザを, 重複も抜けもなく, リアライザ 1 つあたり $O(n)$ 時間で生成する.

研究会等

1. 中野 眞一, 宇野 毅明:
   “On the Enumeration of Colored Trees”, 情報処理学会アルゴリズム研究会, 95, 17-24, 2004 年 5 月.
   概要: A c-tree is a tree such that each vertex has a color $c \in \{c_1, c_2, \cdots, c_m\}$. The problem of enumerating all c-trees with at most n vertices without repetition has an application to data mining problem of tree structured patterns, however no efficient algorithm, which generates each tree in constant time on average, is known. In this paper we give a simple algorithm for enumerating c-trees with at most n vertices and diameter d. Our algorithm generates each c-tree in constant time on average. By using the algorithm for each diameter $2, 3, \cdots, n-1$, we can generate all c-trees with at most n vertices.

学会大会等

1. 宇野毅明:
   “大規模データ処理に対する列挙アルゴリズムの活用”, データ工学ワークショップ, (招待講演), 2005 年 2 月 28 日.

2. 宇野毅明:
   “頻出パターンの高速列挙”, 電気通信情報学会コンピューテーション研究会, (招待講演), 2004 年 12 月 10 日.

3. 清見礼, 宇野毅明, 松井知己:
   “電力取り引きにおける約定量決定問題の高速解法”, 日本オペレーションズリサーチ学会秋季研究発表会, 2004 年 9 月.

C05: 幾つかの画像関連問題の計算複雑度の解析と効率的な解決法の提案

浅野 哲夫　元木 光雄　Arijit Bishnu

北陸先端科学技術大学院大学情報科学研究科
〒 923-1292 石川県能美市旭台町 1-1
{t-asano, mmotoki,arijit}@jaist.ac.jp

最近のディジタルカメラに代表される画像入力装置の普及に伴い、計算機で画像を処理する機会が飛躍的に増大しているが、入力装置の性能向上は必然的にデータ量増大を招き、素朴なアルゴリズムでは妥当な時間内に処理することが困難になりつつある。将来を展望したとき、データ量の爆発により処理不能に陥る危険性があり、今のうちに計算量の理論に基づいて計算困難度を数学的に解析し、それに基づいてアルゴリズムを開発することが急務である。このような観点から，本研究では画像に関連する下記の問題について、本質的な計算複雑度を明らかにするとともに、近似解法を含めて効率の良い現実的な解決法を提案する．
(1) 画像の領域分割：画像に含まれる対象物を最適化の基準に基づいて背景から切り出す問題。
(2) 一様な点配置生成：合理的な尺度の下に指定された長方形領域内に指定個数の点を一様に配置する問題。
(3) 適応型メッシュ生成：変形量に応じたサイズのメッシュを生成する問題。
(4) 高信頼度指紋同定：入力画像に一致する指紋をデータベースから高い信頼性で効率的に探索する問題。

以下，それぞれのテーマについての進捗状況をその成果と共に記す．

1　画像の領域分割

浅野は以前に計算幾何学的な立場から画像の領域分割を行うための効率の良いアルゴリズムを提案しているが，そのときの評価基準は，領域の内外の濃度差を最大にするように領域に分割するというものであった．具体的には，判別分析の基準に基づいてクラス間分散を明度情報を用いて定義し，これを最大にする画像の２分割を求める効率の良いアルゴリズムを開発した．境界線が一つの方向に単調でなければならないという制約はあるものの，調節用のパラメータや経験的な知識に基づいたパラメータ設定が必要ないというのが特徴であった．画像に関する知識が利用できない状況では，意味情報を用いず，明るさの情報だけを用いて自動的に領域分割を行うことは有意義なことであるが，今回はできれば対象画像に関する若干の知識も取り込んだ形で領域分割を行うための方法について考察した．

基本的な考え方は，画像の等高線情報を用いることである．画像の等高線とは，ある一定以上の明るさの領域の境界を様々な明るさについて集めたものである．多くの画像では，明るさ成分だけを取り出して，その典型的な等高線を取り出せば，ほぼ対象画像を認識することができることが計算機実験の結果から分かった．しかし，単なる明るさだけの情報では十分ではないことが多く，色情報も付加した領域分割を考案し，計算機実験を行った．計算機実験の結果は良好であるが，まだ実験で試した例題の数が少ないのが難点であるが，基本的な考え方は固まったので，来年度には実際に計算機上にプログラムを実装して実験を行うとともに，積極的に研究発表も行う予定である．

2　一様な点配置生成と適応型メッシュ生成

様々な応用分野において，平面あるいは空間の指定された領域内に指定された個数の点を一様に

配置する問題があり，様々な分野で様々な方法が提案されている．本研究では，計算幾何学におけるディスクレパンシの理論に基づいて一般的な原理をまず確立し，その上で個別の問題に適用することを計画している．具体的には，ディジタルハーフトーニングとメッシュ生成への応用を念頭に置いている．ディジタルハーフトーニングへの応用に関しては，ネットワークフローの理論や線形計画法などと組み合わせることで，数学的な定式化ができることを示しただけではなく，実際に多項式時間（しかも実際にも高速）のアルゴリズムを示し，実験結果も含めて複数の国際会議において発表した．その結果は，アルゴリズムの専門家だけでなく，産業界からも関心が高く，一部は産業界との共同研究の形に発展する予定である．

メッシュ生成にも重要な応用がある．従来は，乱数などを用いてランダムに点の初期配置を決めてメッシュ生成を行った後で，逐次改善を行うというのが典型的なアプローチである．本研究では，初期配置をディスクレパンシの理論に基づいて注意深く行うことにより，後続の処理の効率と性能を向上させることを目指している．今年度の成果としては，ディスクレパンシ理論に基づく点の初期配置について効率の良い方法を開発するとともに，三角形メッシュに限定したとき，局所的な最適化が直線のアレンジメント上での探索問題に帰着できることを導いたことにある．この成果に基づいて，来年度には実装を行うとともに計算機実験を行い，成果の研究発表も行う予定である．

3　高信頼度指紋同定

指紋の同定は既に実用化されている技術であるが，指紋の同定が各所で行われるにつれ，本質的な問題が浮き彫りになってきている．一つは性能の問題であり，他方は計算速度の問題である．本研究の特徴は，従来画像処理のテクニックだけで行われていた指紋同定に，計算幾何学的手法を導入することである．前処理については，距離変換の技法は非常に有効であることを，理論的にも実験的にも確認し，その成果を複数の国際会議において発表した．この研究に関しては産業界とも意見の交換を行っており，最終的には実用化を目指している．

来年度の計画としては，指の３次元形状と３次元的歪を考慮した特徴点のパターンマッチングについて研究する予定である．現在はその基礎的な考察を行っており，距離変換の概念がここでも役に立ちそうである．次ページ以降に指紋同定に関してまとめたものを掲載しておく．

A Fast Denoising Method for Binary Fingerprint Image

Xuefeng Liand and Tetsuo Asano

ABSTRACT

In this paper we propose a fast method for binary fingerprint image denoising that employs the generalized and ordinary morphological operators based on Euclidian distance transform. This method avoids quite a number of computational redundance. In particular, the computations of denosing step are restricted to a minimum number of pixels. The results show that applying this method on fingerprint image with impulsive noise and useless components yields a segmentation much closer to that of an expect for extracting the minutia accurately.

KEY WORDS

ordinary morphological operator (OMO), generalized morphological operator (GMO), structuring element (SE), strictness, Euclidean distance transform, useless component.

4 Introduction

The performance of fingerprint recognition relies heavily on the quality of the input fingerprint image. However, in practice, due to skin conditions (e.g. wet or dry), sensor noise, incorrect finger pressure, and inherently low-quality fingers, a significant percentage of fingerprint images contains much noise (see (1) in Figure 2.3). The noise of fingerprint image have two categories: they are impulsive noise (salt and pepper noise) and useless components respectively[1]. Several techniques for eliminating the impulsive noise have been developed. Ratha, Chen, and Jain [1] implement a morphological opening whose structuring element is a small box oriented according to the local ridge orientation. Wahab, Chin, and Tan [2] correct the binary image at locations where orientation estimates deviate from their neighboring estimates. This correction is performed by substituting the noisy pixels according to some oriented templates. Ikeda et al. [3] use morphological operators to enhance ridges and valleys in the fingerprint binary image. Since the first two methods consider the orientation, therefore, a fine selection of the directional filters is necessary. Although the third method employs an isotropic constructing element and result keeps the original shape of fingerprint, the impulsive noise can not be eliminated completely. However, time complexity of them are at least $O(n^2 \times d^2)$ for a image with $n \times n$ pixel entries and a filter whose radius is d. It is time consuming. There are few literatures till date with regard to eliminating the useless components. In this paper, we propose a fast and robust method, which employs the generalized and ordinary morphological operators (GMO and OMO) based on distance transform, for eliminating the impulsive noise and useless components, and time complexity can be reduced to $O(l \times d + n^2)$.

The paper is organized as follows: Section 2 reviews the basic conceptions of the mathematical morphology; Section 3 presents a strategy that employs GMO and OMO based on a linear time Euclidean distance transform for denoising; finally, in section 4 the important conclusion is given.

5 Ordinary and generalized morphological operators

5.1 Ordinary morphological operators (OMO)

In mathematical morphology, signal transformations are called morphological filters, which are nonlinear operators that locally modify the geometrical features of signals. Some definitions

[1] Useless component is an object disjoining other objects and whose the largest width is less than the mean width of fingerprint ridges.

are given as follows[5].

Let $B \subset Z^2$ be a simple compact set of small size called structuring element.

Translation:

The translation of a set F by a point x denoted by $F + x$ is defined as:

$$F + x = \{f + x : \exists f \in F\}$$

Where F denote a set of foreground pixels (Black pixels) and F^c denote background (white pixels).

Reflection:

$\breve{B}$ is the reflection of B given by:

$$\breve{B} = \{x : \exists b \in B; x = -b\}$$

Erosion:

The fundamental operation of mathematical morphology is erosion. The erosion of set F by set B is denoted by $F \ominus B$ and is defined by:

$$F \ominus B = \bigcap \{F + b : \exists b \in \breve{B}\}$$

Dilation:

The second most basic operation of binary mathematical morphology is dilation. It is a dual operation to erosion, meaning that it is defined via erosion by set complementarily. The dilation of set F by B is denoted by $F \oplus B$ and is defined by :

$$F \oplus B = \bigcup \{F + b : \exists b \in B\}$$

There are two secondary operations that play a key role in morphological image processing, these being opening and its dual, closing.

Opening:

The opening of image F by image B is denoted by $F \circ B$ and is defined as erosion followed by dilation, namely:

$$F \circ B = (F \ominus B) \oplus B$$

Closing:

The closing of F by B is denoted by $F \bullet B$ and is defined as dilation followed by erosion, namely:

$$F \bullet B = (F \oplus B) \ominus B$$

Some of properties of erosion, dilation, opening and closing are detailed in [5].

From the properties of morphological operators, it is obvious that the shape and size of the structuring element determine the nature and degree of the morphological transformation. The most common structuring elements are horizontal cross, diagonal cross (4-connected set) and 3×3 matrix (8-connected set), respectively (as shown in Figure 2.1).

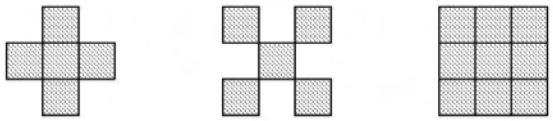


図 2.1: Structuring element: Left (1): Horizontal cross. Middle (2): Diagonal cross. Right (3): 3×3 matrix.

Morphological operators detailed so far, which in the following will be called ordinary morphological operators (OMO), consider only the intersection of the structuring element with the image. Thereby, when a large morphological kernel is used, the OMOs have excessive erosion or dilation. For this reason, it is suggested to define new morphological operators that generalize the ordinary morphological operators, thus achieving control over their strictness. They are described briefly in the following subsection.

5.2 Generalized morphological operators (GMO)

The morphological dilation of F by B can be generalized by combining the size of the intersection into the dilation process. In that sense, a given shift is included in the dilation of F only if the intersection between F and the reflected and shifted B is big enough. The obtained advantage of the generalized dilation is the elimination of

excessive dilation caused by small intersections. That is, the mass of an intersection should be big enough in order to cause a change.

The **generalized dilation** of F by B with strictness s is defined by:

$$F \overset{s}{\oplus} B = \{x : \#(F \bigcap \check{B}) \geq s\}; s \in [1, min(\#F, \#B)]$$

Where # denotes the cardinality of a set.

The ordinary dilation is obtained as a special case of the generalized dilation when $s = 1$.

The **generalized erosion** of F by B with strictness s is defined by:

$$F \overset{s}{\ominus} B = \{x : \#(F^c \bigcap B) < s\}; s \in [1, \#B]$$

Where it is assumed that $\#F < \infty$.

Similarly, the ordinary erosion is also obtained as a special case of generalized erosion when $s = 1$.

The properties of generalized morphological operators can be found in [6].

It is important to note that, using the generalized operators in existing algorithms with strictness greater than one may increase the resistivity of the algorithms to noise and small intrusions.

6 Fingerprint image denoising by Morphological operation based on Euclidean distance transform

6.1 A linear time Euclidean distance transform

We rely on a linear time Euclidean distance transform proposed by Hirata et al. It has two steps.

The step **1** is vertical scan. In a binary image described by set $I_{(n\times n)} \subset Z^2$, for each foreground pixel $p(i,j) \in F$, compute its vertical distance $d^v_{i,j}$, which is the distance to the nearest background points $p(i,j) \in F^c$ in the same column, by vertical direction scan. The time complexity is bounded by $2n^2$.

The step **2** is horizontal scan. In this step, we draw a collection of parabolas $\{p_j | j = 1...n\}$ for each $p(i,j) \in F$ in the same row. The x and y coordinates of a parabola's origin are j and the vertical distance $d^v_{i,j}$ of corresponding pixel $p(i,j) \in F$ respectively. Then, compute the lower envelope of the collection, which is a sequence of parabolas $\{p_{j'} | j' = k; k \in n\}$. At this time, each $p(i,j) \in F$ in the row i $(i \in n)$, is associated with a new parabola $p_{j'}$ that is contributed by j' and $d^v_{i,j'}$ of $p(i,j') \in F$. Finally, the Euclidean distance $d_{i,j}$ of $p(i,j) \in F$ is equal to $\sqrt{{d^v_{i,j'}}^2 + (j'-j)^2}$. The time complexity of this step is bounded by $4n^2$.

Therefor, this Euclidean distance transform is a linear time algorithm.

6.2 Morphological operation based on Euclidean distance transform

Symmetrical and circular structuring elements (SE) play a fairly central role in mathematical morphology in the continuous plane, since they provide an isotropic treatment of the image. On the other hand, for digital images, circular SE are rarely used because there is no such a SE on a discrete lattice. Indeed, a direct application of the definition above leads to a computation cost of complexity $O(n^2 \times d^2)$ for an image of size $n \times n$ and a SE of radius d.

According to the properties of morphological operators, computing these morphological operations of a set F, only the edge of this set needs to be considered. More accurately, we have

$$F \ominus B = F \bigcap (\partial(F) \ominus B)$$

$$F \oplus B = F \bigcup (\partial(F) \oplus B)$$

where $\partial(F)$ is the edge of F, that is the set of pixels of F with at least a direct neighbor not belonging to F. If l is the length of the contour of F, that is the cardinal of set $\partial(F)$, then the

computational complexity is reduced to $O(l \times d^2)$ for any SE of radius d, obviously $l \leq \frac{n^2}{2}$, plus n^2 time to check whether the pixels belong to $\partial(F)$, or not.

When B is a ball, it can be defined as

$$B = \{b : d(b, 0) \leq d\}$$

where $d(b, F)$ is the distance from pixel b to the set F, that is the distance from pixel b to the nearest pixel belonging to F. For instance, horizontal cross can be defined by $d(b, 0) = 1$; diagonal cross is $d(b, 0) = 1.414$; 3×3 matrix is $1 \leq d(b, 0) \leq 1.414$ (as shown in Figure 2.2), and so on so far. More intuitively, for example (1), whenever the value of center is 1, that means at least one of its four neighbors has a different state. It is similar to others.

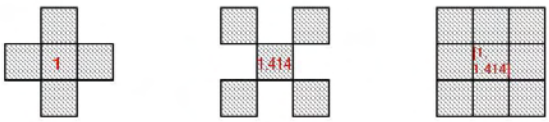


図 2.2: Structuring element defined by distance value: Left (1): Horizontal cross ($d(b, 0) = 1$). Middle (2): Diagonal cross ($d(b, 0) = 1.414$). Right (3): 3×3 matrix ($1 \leq d(b, 0) \leq 1.414$).

Then, erosion and dilation by B can also be expressed as the threshold of a distance function, i.e.

$$F \ominus B = \bigcap \{F - b : d(b, F) \leq d\}$$

$$F \oplus B = \bigcup \{F + b : d(b, F) \leq d\}$$

In practise, morphological operators only deal with the pixels whose distance transform value is not greater than d. If the strictness of generalized morphological operations is greater than 1, operators should count the number of different states of neighbors. In this case, time complexity of operation is $O(l \times d^2)$. But OMO, i.e. strictness is 1, needn't check the states of neighbors, then the complexity is further reduce to $O(l)$.

6.3 Denoising by GMO and OMO based on distance transform

In practice, due to skin conditions (e.g. wet or dry), sensor noise, incorrect finger pressure, fingerprint image obtained from sensor contains much noises, they heavily affect the accuracy of further processing. The noises of fingerprint image have many shapes and directions. Thus, a fine selection of the directional ordinary morphological operators is required; a large morphological kernel may be required. In such cases, effects of noise may damage the expected results due to extreme strictness of the OMO. The GMOs, however, have controllable strictness and so excessive erosion and dilation may be prevented. In other hand, due to controlling the strictness of GMO rather than its shape, A GMO can adapt itself to the orientation and shape of fingerprint without adopting amount of directional operators.

Use of GMO

Since the impulsive noise is fairly small and thin, a square SE of 3×3 pixels (corresponding to $1 \leq d_{i,j} \leq 1.414$) with strictness of 3 is used. Then, the processing steps of this phase are following:

1. **Implement Euclidean distance transform.**
2. **Pick up all pixels whose distance value are 1 or 1.414 and do generalized opening with strictness of 3 on these pixels.**
3. **Update the distance values. Go to step 2.**

Step 2, 3 were repeated until the opening is idempotent. Generally speaking, 3 loops are sufficient for fingerprint image. Owing to the linear time distance transform, time complexities of step 1 and 3 are $O(n^2)$. And step 2 takes $O(l \times d) + n^2$ time.

Experimental results are shown in Figure 2.3 when a generalized opening is applied to the image. Result shows the image is fairly clean and fingerprint is less affected. Moreover, one considerable thing is with the use of GMO it needn't apply a closing to refill, as happens with the OMO. Thus, with GMO is possible to carry out less quantity of operations than with OMO. However, there are some useless component are remained.

図 2.3: Eliminating the impulsive noise. Left (1): original Image. Right (2): opening with a SE of 3×3 pixels and strictness 3.

Use of OMO

Definition *Useless component is an object disjoining other objects and whose the largest width*[2] *is less than the mean width of fingerprint ridges and much greater than impulsive noise's.*

One strategy can be used, i.e. we take information from the image with useless components (for example (1) in Figure 2.4) and the processed image in which useless components are eliminated completely but fingerprint can not totally be deleted although they are affected in some measure ((2) in Figure 2.4). Then integrate them for restoring expected image without useless components. Since it is not necessary keeping the shape of fingerprint in processed image. An ordinary erosion is sufficient for this process. Meanwhile, it is also determined by the correct selection of the SE as well as its size.

Lemma *When an isotropic SE satisfies the following condition:*

$$max(W_{useless}) \leq 2d \leq mean(W_{ridge})$$

the useless components can be eliminated, but some of skeletons of fingerprint shall be remained, where $W_{useless}$ and W_{ridge} are widths of useless component and fingerprint ridge, respectively. d is radius of SE.

PROOF. According to the erosion of ordinary morphology, eroding an object can be found by intersecting all translates of the object by the reflection of the SE. As assumption, the diameter of isotropic SE is not less than the maximal width of useless component. Then the object translated by the reflection of SE is too far to intersect any other translated object, i.e. $\bigcap\{F - b : b \exists B\} = \phi$. Thus, the useless components can be eliminated under such condition. The diameter $2d$, however, is not greater than the mean width of fingerprint. That means some wider portions, which are wider than SE, are not translated so far that they can intersect others. So, some of skeletons of fingerprint are remained.

Therefor, according to this aim we carried out the operation in the following way: the image ((1) in Figure 2.4) is deal with by an ordinary erosion using a circular SE of 13 pixels (corresponding to $1 < d_{i,j} \leq 2$)[3]. Following this way, an image ((2) in Figure 2.4) is obtained without useless components completely. Due to an ordinary operation, the time complexity is only $O(l) + n^2$. Consequently, image obtained from previous phase is marked and it is established a correspondence between both images. The marked objects which do not correspond with some information in the eroded image are classified as useless components and, therefore, they

[2]Central line l_c of an object is a line which minimizes the summation of square distances of points on the object to this line. So, the length of a object is the length of central line. Given a point p lies on central line l_c, width of object at p is the length of the straight line segment, which passes through p and perpendicular to l_c and whose two end points are boundary points of object.

[3]Since the width of fingerprint ridge is about 5 pixels wide, the circular SE of 13 pixels is a good choice.

are eliminated. The rest marked objects which

図 2.4: Eliminating the useless components. Top left (1): an image with useless components. Top right (2): Eroded image with SE of 13 pixels. Bottom (3): the output image.

correspond to information are classified as fingerprint, remaining finally in the output image ((3) in Figure 2.4).

The eliminating useless component algorithm by ordinary erosion based on Euclidean distance transform is given as follows:

Given: a binary image $I_(n \times n)$ with useless components and eroded image I'. $p(i,j) \in I; p'(i,j) \in I'$**.**

Output: image without useless components completely.

{Q is a queue.}

BEGIN

For i,j = 1 to n

If $p(i,j) \in F$ **and not visited**

Push($p(i,j)$**), count = 0**

1 Mark useless components

While Q is not empty

Pop($p(i,j)$**), label** $p(i,j)$ **visited**

If any neighbor of $p(i,j)$ **is in** F **and not visited**

Push it into Q and label it visited

If $p'(i,j) \in F$ **then count++**

2 Eliminate useless component

If count == 0

Push($p(i,j)$**)**

While Q is not empty

Pop($p(i,j)$**), let** $p(i,j) \in F^c$

If any neighbor of $p(i,j)$ **is in** F

Push it into Q

END.

Time complexity of eliminating useless components algorithm.

- Because $p(i,j)$ is pushed and popped only once, Step 1 takes n^2 time to mark useless components.
- Step 2 is similar to step 1. Thus, it takes n^2 time for eliminating useless components.

It is clear that time complexity is $O(n^2)$.

7 Conclusion

We proposed a fast method using GMO and OMO based on Euclidean distance transform to eliminate the impulsive noise and useless components from fingerprint image. As above introduction, it is observed that the Euclidean distance transform is $O(n^2)$; eliminating impulsive noise by GMO is $O(l \times d)+n^2$, where $d = 2$; eroding image for eliminating useless components is $O(l)+n^2$; finally, eliminating useless components is $O(n^2)$. Thus, the whole processes is a efficient and robust method, rather than $O(n^2 \times d^2)$ of conventional methods.

Since the GMO has controllable strictness which leads to less sensitivity to noise, the experimental results presented in Section 3 are quite satisfactory.

参考文献

[1] N.K. Ratha, S.Y. Chen and A.K. Jain, Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images, *Pattern Recognition*, Vol. 28, no. 11, 1995, 1657-1672.

[2] A. Wahab, S.H. Chin and E.C. Tan, Novel Approach to Automated Fingerprint Recognition, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 145, no. 3, 1998, 160-166.

[3] N. Ikeda et al, Fingerprint Image Enhancement by Pixel-Parallel Processing, *Proc. Int. Conf. on pattern recognition (16th)*, Vol. 3, 2002, 752-755.

[4] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, *Handbook of Fingerprint Recognition,*(New York: Springer-Verlag, 2003).

[5] J. Serra and P. Soille, *Mathematical Morphology and its Applications to Image Processing,*(Kluwer Academic Publishers, 1994).

[6] G. Agam and Its'hak Dinstein, Generalized Morphological Operators Applied to Map-Analysis, *In Proceedings of SSPE'96*, 1995, 60-69.

[7] J.C. Russ, *The Image Processing Handbook (Third Edition),*(CRC Press LLC, 1999).

Distributing Distinct Integers Uniformly over a Square Matrix with Application to Digital Halftoning

T. Asano, S. Choe, S. Hashima, Y. Kikuchi, and S-C. Sung

Abstract

This paper considers how to distribute n^2 integers between 0 and n^2-1 as uniformly as possible over an $n \times n$ square matrix. We introduce a discrepancy-based measure to evaluate the uniformity. More precisely, we take a sum of matrix elements over every $k \times k$ contiguous submatrix and define the discrepancy of the matrix as the largest difference among those sums. It is known that if n and k are both even integers then we can construct zero-discrepancy matrices. In this paper we present a scheme for achieving a new discrepancy bound $2n$ when n is odd and k is 2. This is an improvement from the previous bound $4n$. We borrow basic ideas behind orthogonal Latin squares and semi-magic squares. An n-ary number system also plays an important part.

This problem is closely related to digital halftoning. Low discrepancy matrices would improve the quality of commonly used Ordered Dither Algorithm.

8 Introduction

Digital Halftoning is an important technique for the rendition of continuous-tone pictures on displays that can only produce two levels. There have been a great number of methods for digital halftoning. One of the most popular methods is *Ordered Dithering* which determines an output level at each pixel by comparison with a threshold in a predetermined table called *Dither Matrix*. The performance of the algorithm heavily depends on the Dither matrix.

A Dither matrix is an $n \times n$ square matrix containing integers $0, \ldots, n^2 - 1$. It is good when those integers are *uniformly* distributed. To evaluate the uniformity we introduce a discrepancy-based measure. More precisely, we take a sum of matrix elements over every $k \times k$ contiguous submatrix (region) and define the discrepancy of the matrix as the largest difference among those sums. This measure reflects human eye perception usually modeled using weighted sum of intensity levels with Gaussian coefficients over square regions around each pixel [2]. It is known by experience that a matrix with low discrepancy frequently produces good-looking pictures. This is the reason why we are interested in finding a good matrix with low discrepancy.

The analogous geometric problem of distributing n points uniformly in a unit square has been studied extensively in the literature [6, 9]. Usually, a family of regions is introduced to evaluate the uniformity of a point distribution. If the points of an n-point set P are uniformly distributed, for any region R in the family the number of points in R should be close to $\frac{1}{n}\,\mathrm{area}(R)$, where $\frac{1}{n}$ is the point density of P in the entire square. Thus, the *discrepancy of P in a region R* is defined as the difference between this value and the actual number of points of P in R. The *discrepancy of the point distribution P* with respect to the family of regions is defined by the maximum such difference, over all regions. The problem of establishing discrepancy bounds for various classes of regions has been studied extensively [7]. One of the simplest families is that of axis-parallel rectangles for which $\Theta(\log n)$ bound is known [6, 9].

For the problem of establishing discrepancy bounds for families of regions (contiguous submatrices), some preliminary observations are obtained in [1]. One basic observation is that we can construct an $n \times n$ matrix of zero-discrepancy for a family of 2×2 regions if n is even. A space-efficient algorithm is also presented in [1] for constructing a $k^m \times k^m$ matrix of zero-discrepancy for a family of $k \times k$ regions. More precisely, given any matrix index (i, j) we can compute the corresponding matrix element of the index in constant time using only $O(k^2)$ working space instead of $O(k^{2m})$ required to store an output matrix. It is also shown in [1] that zero-discrepancy cannot be achieved if n is odd and k is even, and only trivial bound has been obtained for the discrepancy in that case. In this paper we present a new scheme for achieving a new discrepancy bound $2n$ when $n \geq 5$ is odd and k is 2. This is an improvement from the previous bound $4n$ [1]. Basic tools and theories are orthogonal Latin squares, semi-magic squares, and the n-ary number system.

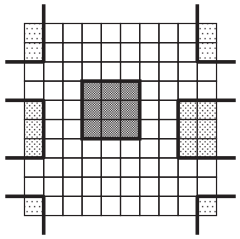


図 2.5: 3×3 contiguous submatrices (regions).

9 Preliminary Definitions

For integers $n > 1$, let $\mathbb{Z}_n(n)$ be the class of all $n \times n$ integer matrices such that all the integers ranging from 0 to $n - 1$ are included exactly n times and let $\mathbb{Z}_1(n)$ be that of all $n \times n$ matrices which contain every value $0, \ldots, n^2 - 1$ exactly once. In this paper we only deal with square matrices consisting of an odd number of rows (and columns) unless otherwise specified.

Given an $n \times n$ matrix $P = (p_{i,j})$ and a region $R \subseteq \{0, \ldots, n-1\}^2$, $P(R)$ denotes the sum of the elements of P in locations given by R, i.e., $P(R) = \sum_{(i,j)\in R} p_{i,j}$. A *contiguous $k \times k$ region* $R_{i,j}^{(k)} \subseteq \{0, \ldots, n-1\}^2$ with its upper left corner at (i, j) is defined by $R_{i,j}^{(k)} = \{(i', j') \mid i' = i, \ldots, i + k - 1 \text{ and } j' = j, \ldots, j + k - 1\}$, where

indices are calculated modulo n. Fig. 2.5. [4] The *$k \times k$-discrepancy* of an $n \times n$ matrix P for the family $\mathcal{F}_{k,n}$ of all $k \times k$ regions is defined as

$$\max_{R \in \mathcal{F}_{k,n}} P(R) - \min_{R' \in \mathcal{F}_{k,n}} P(R').$$

Let $\mathbb{N}(k,n)$ be the set of all such zero-$k \times k$-discrepancy matrices of order (k,n).

Theorem 1 *[1] The set $\mathbb{N}(k,n)$ of zero-$k \times k$-discrepancy matrices of order (k,n) has the following properties:*

(a) $\mathbb{N}(k,n)$ is non-empty if k and n are both even.

(b) $\mathbb{N}(k,n)$ is empty if k and n are relatively prime.

(c) $\mathbb{N}(k,n)$ is empty if k is odd and n is even.

(d) $\mathbb{N}(k,k^m)$ is non-empty for any integers k and m, $k \geq 2, m \geq 2$.

It follows from the theorem that zero-discrepancy cannot be achieved in a basic case of n odd and k even. In this paper we consider how much we can reduce the discrepancy of such a matrix in this basic case. One simple question is whether we can achieve a $\Theta(\log n)$ bound as in geometric discrepancy problems.

10 Basic Construction Schemes

A goal here is to design a low discrepancy matrix. We begin with some basic schemes for constructing matrices having some nice properties.

10.1 n-Ary Number System

From now on, we assume that n is an odd number not less than 3, and our target $n \times n$ matrix $C \in \mathbb{Z}_1(n)$. Since all such integers ranging from 0 and n^2-1 can be represented by two digits in the n-ary number system, we can associate to each $C \in \mathbb{Z}_1(n)$ two square matrices A and B representing upper and lower digits. That is, each element $c_{i,j}$ of the matrix C is given by

$$c_{i,j} = n \times a_{i,j} + b_{i,j},$$
$$0 \leq a_{i,j}, b_{i,j} < n,\ i,j = 0,1,\ldots,n-1.$$

Observe that $C \in \mathbb{Z}_1(n)$ if and only if the two matrices A and B are in the class $\mathbb{Z}_n(n)$ and are mutually orthogonal, that is, no ordered pair $(a_{i,j}, b_{i,j})$ occurs more than once. So, we need schemes for generating two mutually orthogonal matrices in the class $\mathbb{Z}_n(n)$.

In the following, we first propose two schemes called *Alternating Diagonal Sequencing* and *Diagonal Repeating*, and then propose another scheme obtained based on the first two scheme.

10.2 Alternating Diagonal Sequencing

Alternating Diagonal Sequencing is a scheme for generating a matrix $A_n = (a_{i,j})$ in the class $\mathbb{Z}_n(n)$ as follows.

$$a_{i,j} = \begin{cases} i & \text{if } i+j \text{ is odd,} \\ n-1-i, & \text{otherwise.} \end{cases}$$

Recall that $R^{(2)}_{i,j} = \{(i,j),(i+1,j),(i,j+1),(i+1,j+1)\}$ is the 2×2 contiguous region on an $n \times n$ matrix, and $A_n(R^{(2)}_{i,j})$ is the sum of elements of A_n in the region $R^{(2)}_{i,j}$, that is,

$$A_n(R^{(2)}_{i,j}) = a_{i,j} + a_{i+1,j} + a_{i,j+1} + a_{i+1,j+1}.$$

By definition and the fact that n is odd, we have

$$a_{i,j}+a_{i,j+1} = \begin{cases} 2i & \text{if } i \text{ odd, } j = n-1, \\ 2n-2-2i & \text{if } i \text{ even, } j = n-1, \\ n-1 & \text{otherwise.} \end{cases}$$

Hence, we have

$$A_n(R^{(2)}_{i,j}) = \begin{cases} 2n & \text{if } i < n-1 \text{ even, } j = n-1, \\ 2n-4 & \text{if } i \text{ odd, } j = n-1, \\ 2n-2 & \text{otherwise.} \end{cases} \quad (2.23)$$

[4] Throughout this paper, index arithmetic is performed modulo matrix size n unless otherwise noted.

Let $\hat{A}_n = (\hat{a}_{i,j})$ be an $n \times n$ matrix defined by

$$\hat{a}_{i,j} = a_{j,n-1-i}, \text{ for each } i, j = 0, \ldots, n-1.$$

Roughly speaking, $\hat{A}_n$ can be obtained by a clockwise 90 degree rotation of A_n. Thus, we have

$$\hat{A}_n(R^{(2)}_{i,j}) = \begin{cases} 2n-4 & \text{if } i = n-1,\ j < n-1 \text{ even}, \\ 2n & \text{if } i = n-1,\ j \text{ odd}, \\ 2n-2 & \text{otherwise.} \end{cases} \tag{2.24}$$

Lemma 2 *The matrix $nA_n + \hat{A}_n$ belongs to $\mathbb{Z}_1(n)$.*

Proof: First, it is obvious that all elements in $nA_n + \hat{A}_n$ are integers ranging from 0 to $n^2 - 1$. Then, to complete the proof, each integer ranging from 0 to n^2-1 appears exactly once in $nA_n + \hat{A}_n$.

Suppose there are two locations $(i,j), (i',j') \in \{0,1,\ldots,n-1\}^2$ such that $na_{i,j} + \hat{a}_{i,j} = na_{i',j'} + \hat{a}_{i',j'}$. It follows that $a_{i,j} = a_{i',j'}$ and $\hat{a}_{i,j} = \hat{a}_{i',j'}$. By definition, each $a_{i,j}$ is either i or $n-1-i$. From $a_{i,j} = a_{i',j'}$, we have $i' = i$ if $i+j$ and $i'+j'$ have the same parity, and $i' = n-1-i$ otherwise. On the other hand, we have $a_{j,n-1-i} = a_{j',n-1-i'}$ from $\hat{a}_{i,j} = \hat{a}_{i',j'}$. Then, we have $j' = j$ if $i+j$ and $i'+j'$ have the same parity, and $j' = n-1-j$ otherwise.

As a consequence, $i+j$ and $i'+j'$ have the same parity. Otherwise, $i+j+i'+j'$ must be an odd, however, $i+j+i'+j' = i+j+(n-1-i)+(n-1-j) = 2n-2$. Hence, $i' = i$ and $j' = j$. Therefore, we can conclude that each integer ranging from 0 to n^2-1 appears exactly once in $nA_n + \hat{A}_n$, i.e., $nA_n + \hat{A}_n \in \mathbb{Z}_1(n)$. □

Lemma 3 *The 2×2 discrepancy of $nA_n + \hat{A}_n$ is $4n$.*

Proof: Observe from (2.23) and (2.24) that there is no pair (i,j) such that $A_n(R^{(2)}_{i,j})$ and $\hat{A}_n(R^{(2)}_{i,j})$ are both $2n$ or both $2n-4$. Hence, the 2×2 sums of $nA_n+\hat{A}_n$ is at most $2n\times n+2n-2 = 2n^2+2n-2$ and are at least $(2n-4)\times n + 2n - 2 = 2n^2 - 2n - 2$. Indeed, $nA_n(R^{(2)}_{0,n-1}) + \hat{A}_n(R^{(2)}_{0,n-1}) = 2n^2+2n-2$ and $nA_n(R^{(2)}_{1,n-1}) + \hat{A}_n(R^{(2)}_{1,n-1}) = 2n^2-2n-2$. Therefore, the 2×2 discrepancy of $nA_n + \hat{A}_n$ is $4n$. □

Observe that, when n is even, the 2×2 discrepancy of $nA_n + \hat{A}_n$ becomes 0, because we have $A_n(R^{(2)}_{i,j}) = \hat{A}_n(R^{(2)}_{i,j}) = 2n-2$ for every (i,j) when n is even. Notice that the non-emptyness of $\mathbb{N}(2,n)$ for even n is already shown in (a) of Theorem 1.

10.3 Diagonal Repeating

We now define another scheme called *Diagonal Repeating* for generating low discrepancy matrices. We partition the n^2 locations of an $n \times n$ matrix into n disjoint regions $L^{(+)}_0, \ldots, L^{(+)}_{n-1}$ along 45 degree lines as follows:

$$L_s = \{(i,j) \mid (i+j) \bmod n = s\}, \text{ for } s = 0, \ldots, n-1.$$

We define an $n \times n$ matrix $D_n = (d_{i,j})$ as follows:

$$d_{i,j} = \begin{cases} s & \text{if } (i,j) \in L_s,\ s \text{ even}, \\ n-1-s & \text{if } (i,j) \in L_s,\ s \text{ odd}. \end{cases}$$

For example, when $n = 5$, we have

$$D_5 = \begin{pmatrix} 0 & 3 & 2 & 1 & 4 \\ 3 & 2 & 1 & 4 & 0 \\ 2 & 1 & 4 & 0 & 3 \\ 1 & 4 & 0 & 3 & 2 \\ 4 & 0 & 3 & 2 & 1 \end{pmatrix}.$$

Observe that the same number is repeated along 45 degree lines. So, it is called *Diagonal Repeating.*

By definition, we have

$$d_{i,j}+d_{i,j+1} = \begin{cases} n-2 & \text{if } (i,j) \in L_s,\ s < n-1 \text{ even}, \\ n & \text{if } (i,j) \in L_s,\ s \text{ odd}, \\ n-1 & \text{otherwise.} \end{cases}$$

Hence, we have

$$D_n(R^{(2)}_{i,j}) = \begin{cases} 2n-1 & \text{if } (i,j) \in L_{n-2}, \\ 2n-3 & \text{if } (i,j) \in L_{n-1}, \\ 2n-2 & \text{otherwise.} \end{cases} \tag{2.25}$$

Let $\hat{D}_n = (\hat{d}_{i,j})$ be an $n \times n$ matrix defined by

$$\hat{d}_{i,j} = d_{j,n-1-i}, \text{ for each } i, j = 0, \ldots, n-1.$$

Here, $\hat{D}_n$ can be obtained by a clockwise 90 degree rotation of D_n. Analogous to L_ss, we define sets $L'_0, \ldots, L'_{n-1}$ along -45 degree lines:

$$L'_s = \{(i,j) \mid (j-i) \bmod n = s\}, \text{ for } s = 0, \ldots, n-1.$$

Then, $\hat{D}_n = (\hat{d}_{i,j})$ can be defined in terms of L'_ss as follows.

$$\hat{d}_{i,j} = \begin{cases} n-1-s & \text{if } (i,j) \in L'_s, \ s \text{ even}, \\ s & \text{if } (i,j) \in L'_s, \ s \text{ odd}. \end{cases}$$

Moreover, we have

$$\hat{D}_n(R^{(2)}_{i,j}) = \begin{cases} 2n-1 & \text{if } (i,j) \in L'_0, \\ 2n-3 & \text{if } (i,j) \in L'_{n-1}, \\ 2n-2 & \text{otherwise.} \end{cases} \quad (2.26)$$

Lemma 4 *The matrix $nD_n + \hat{D}_n$ belongs to $\mathbb{Z}_1(n)$.*

Proof: Again, it is obvious that all elements in $nD_n + \hat{D}_n$ are integers ranging from 0 to $n^2 - 1$. Then, to complete the proof, each integer ranging from 0 to $n^2 - 1$ appears exactly once in $nD_n + \hat{D}_n$.

Recall that n is odd. Then, for every two pairs (i,j) and (i',j'), $d_{i,j} = d_{i',j'}$ if and only if $(i+j) \bmod n = (i'+j') \bmod n$, and $\hat{d}_{i,j} = \hat{d}_{i',j'}$ if and only if $(j-i) \bmod n = (j'-i') \bmod n$. Moreover, the two sets L_s and L'_t intersect at a single location for every $s, t = 0, \ldots, n-1$. Hence, for every two pairs (i,j) and (i',j'), $nd_{i,j} + \hat{d}_{i,j} = nd_{i',j'} + \hat{d}_{i',j'}$ if and only if $i = i'$ and $j = j'$. Therefore, we can conclude that each integer ranging from 0 to $n^2 - 1$ appears exactly once in $nD_n + \hat{D}_n$, i.e., $nD_n + \hat{D}_n \in \mathbb{Z}_1(n)$. □

The following lemma shows that Diagonal Repeating can produce lower discrepancy matrices than Alternating Diagonal Sequencing.

Lemma 5 *The 2×2 discrepancy of $nD_n + \hat{D}_n$ is $2n+2$.*

Proof: From (2.25) and (2.26), the maximum and minimum 2×2 sums of $D_n(R^{(2)}_{i,j})$s are respectively $D_n(R^{(2)}_{n-1,n-1}) = (2n-1) \times n + 2n - 1 = 2n^2 + n - 1$ and $D_n(R^{(2)}_{0,n-1}) = (2n-3) \times n + 2n - 3 = 2n^2 - n - 3$. □

The discrepancy bound $2n+2$ achieved by Diagonal Repeating is much better than the bound $4n$ done by Alternating Diagonal Sequencing. Unfortunately, this bound is not optimal. In fact, we reduce the discrepancy bound further to $2n$ in the next section. Nevertheless, this bound looks near optimal because of the following theorem establishing a lower bound 2 on the 2×2 discrepancy for matrices in the class $\mathbb{Z}_n(n)$. In fact, the theorem shown a stronger result.

Theorem 6 *Let k be any integer such that $2 \leq k < n$. If n and k are relatively prime, then the $k \times k$ discrepancy of each $A \in \mathbb{Z}_n(n)$ is at least 2.*

Proof: Let $A \in \mathbb{Z}_n(n)$. Observe that each matrix element is included in exactly k^2 different $k \times k$ regions, and each integer between 0 and $n-1$ appears exactly n times in A. Thus,

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} A(R^{(2)}_{i,j}) = k^2(0 + 1 + \cdots + n - 1) \times n$$
$$= k^2 n^2 \tfrac{(n-1)}{2}.$$

The lemma is proven by contradiction.

Suppose the $k \times k$ discrepancy of A is 0 for some $A \in \mathbb{Z}_n(n)$. It follows that that every $k \times k$ region has the same sum $k^2(n-1)/2$. Define a row sum $r_{i,j}$ by $r_{i,j} = a_{i,j} + \cdots + a_{i,j+k-1}$. In terms of $r_{i,j}$s, we have $r_{i,j} + r_{i+1,j} + \cdots + r_{i+k-1,j} = k^2(n-1)/2$ for $i, j = 0, 1, \ldots, n-1$, which implies $r_{i,j} = r_{i+k,j}$. Since n and k are relatively prime, we have $r_{i,0} = r_{i,1} = \cdots = r_{i,n-1}$ for each $i = 0, 1, \ldots, n$, and thus, $r_{i,j} = k(n-1)/2$ for each $i, j = 0, 1, \ldots, n-1$. By applying the same arguments to elements of A, it follows that all the elements of the matrix A are $(n-1)/2$, which contradicts to the assumption $A \in \mathbb{Z}_n(n)$.

Next, suppose the $k \times k$ discrepancy of A is 1 for some $A \in \mathbb{Z}_n(n)$. Then, there are only two different $k \times k$ sums S_0 and S_1 with $S_1 = S_0 + 1$. For $k = 0, 1$, we denote by R_k the number of $k \times k$ regions whose sums are S_k. Then, we have $R_0 + R_1 = n^2$ and $0 < R_0, R_1 < n^2$. Then, we have $R_0 S_0 + R_1 S_1 = k^2 n^2 (n-1)/2$. From $R_0 + R_1 = n^2$ and $S_1 = S_0 + 1$, we have

$$R_1 = k^2 n^2 \frac{(n-1)}{2} - n^2 S_0 = n^2 \left(k^2 \frac{(n-1)}{2} - S_0 \right).$$

Since n is odd and S_0 is an integer, R_1 is a multiple of n^2, which contradicts $0 < R_1 < n^2$. □

Observe from (2.25) that D_n has 2×2 discrepancy 2, and according the theorem, D_n has the lowest 2×2 discrepancy among all matrices in $\mathbb{Z}_n(n)$.

11 Combined Strategy for Improving Discrepancy

We have presented two schema for generating low discrepancy matrices, i.e., Alternating Diagonal Sequencing and Diagonal Repeating. The discrepancy bound achieved is $2n + 2$ for those matrices in the class $\mathbb{Z}_1(n)$ with n odd. In this section we propose yet another scheme, called *Modified Alternating Diagonal Sequencing*, based on these two strategies to achieve a better bound, $2n$.

Here we take D_n as the matrix for upper digits, which has the lowest 2×2 discrepancy among all matrices in $\mathbb{Z}_n(n)$. Recall that all the elements of D_n in the location given by L_s have the same value (for each $(i,j) \in L_s$, $d_{i,j} = s$ if s is even, and otherwise $d_{i,j} = n - 1 - s$).

For lower digits, we take the matrices $M_n = (m_{i,j})$ defined as follows:

$$m_{i,j} = \begin{cases} i & \text{if } (i,j) \in L_1, \\ i & \text{if } (i,j) \in L_s,\ s \geq 2,\ s \text{ even}, \\ n-1-i & \text{otherwise}, \end{cases}$$

For example, when $n = 5$,

$$M_5 = \begin{pmatrix} 4 & 0 & 0 & 4 & 0 \\ 1 & 1 & 3 & 1 & 3 \\ 2 & 2 & 2 & 2 & 2 \\ 1 & 3 & 1 & 3 & 3 \\ 4 & 0 & 4 & 4 & 0 \end{pmatrix}.$$

By the definition of M_n, for each $s = 0, \ldots, n-1$, all elements of the matrix M_n in the locations given by L_s have different values, i.e., on matrix M_n, each of $0, \ldots, n-1$ appears exactly once in the locations given by L_s. This proof the following lemma.

Lemma 7 *The matrices $nD_n + M_n$ belongs to $\mathbb{Z}_1(n)$.*

Now we estimate the 2×2 discrepancy of $nD_n + M_n$. Recall that we have

$$D_n(R^{(2)}_{i,j}) = \begin{cases} 2n-1 & \text{if } (i,j) \in L_{n-2}, \\ 2n-3 & \text{if } (i,j) \in L_{n-1}, \\ 2n-2 & \text{otherwise}, \end{cases}$$

Moreover, by definition, we have

$$m_{i,j} + m_{i,j+1} = \begin{cases} 2i & \text{if } (i,j) \in L_1, \\ n-1 & \text{otherwise}, \end{cases}$$

and thus, $M_n(R^{(2)}_{i,j}) =$

$$\begin{cases} n + 2i + 1 & \text{if } (i,j) \in L_0 \text{ and } i < n-1, \\ n-1 & \text{if } (i,j) \in L_0 \text{ and } i = n-1, \\ n + 2i - 1 & \text{if } (i,j) \in L_1, \\ 2n-2 & \text{otherwise}. \end{cases}$$

Then, we obtain the following theorem.

Theorem 8 *The 2×2 discrepancy of the matrix $nD_n + M_n$ is $2n$ when $n > 3$.*

Proof: Assume that $n > 3$. Then, from $n - 2 > 1$,

$(nD_n + M_n)(R^{(2)}_{i,j}) =$

$$\begin{cases} 2n^2 - n + 2i + 1 & \text{if } (i,j) \in L_0 \text{ and } i < n-1, \\ 2n^2 - n - 1 & \text{if } (i,j) \in L_0 \text{ and } i = n-1, \\ 2n^2 - n + 2i - 1 & \text{if } (i,j) \in L_1, \\ 2n^2 + n - 2 & \text{if } (i,j) \in L_{n-2}, \\ 2n^2 - n - 2 & \text{if } (i,j) \in L_{n-1}. \\ 2n^2 - 2 & \text{otherwise}. \end{cases}$$

Hence, the largest and the smallest 2×2 sums in $nD_n + M_n$ are respectively $2n^2 + n - 2$ (on L_{n-2}) and $2n^2 - n - 2$ (on L_{n-1}), and thus, the 2×2 discrepancy is $2n$. □

12 Conclusions

In this paper we have introduced a discrepancy-based measure to evaluate a class of integer-valued matrices for application to digital halftoning. In the context of digital halftoning, a problem is defined on a discrete plane instead of a continuous plane used in the traditional discrepancy theory. We are also required to fill in lattice points by distinct integers instead of just placing points on the continuous plane. We have observed that discrepancy is affected by integral properties between a matrix size n and a region size k.

We have devoted to minimizing the discrepancy against a family of 2×2 regions. The region size may be too small for practical application to digital halftoning. We could define a combined discrepancy measure, that is, sum of discrepancy bounds for several families of regions such as $\mathcal{D}_{2,n}(P) + \mathcal{D}_{3,n}(P) + \cdots + \mathcal{D}_{k,n}(P)$. What is know so far is that there is no matrix P for which the combined discrepancy bound $\mathcal{D}_{2,n}(P) + \mathcal{D}_{3,n}(P)$ is zero.

One technical open problem is to prove optimality of the discrepancy bound $2n$ we have established in this paper. It is not so easy even for a small value of n. For example, when n is five, we have 24! different matrices to check.

参考文献

[1] B. Aronov, T.Asano, Y. Kikuchi, S. C. Nandy, S. Sasahara, and T. Uno: "A Generalization of Magic Squares with Applications to Digital Halftoning," to appear in Proc. of International Symposium on Algorithms and Computation, Hong Kong, December, 2004.

[2] T. Asano, "Digital Halftoning: Algorithm Engineering Challenges," *IEICE Trans. on Inf. and Syst.*, E86-D, 2, 159–178, 2003.

[3] T. Asano, N. Katoh, K. Obokata, and T. Tokuyama, "Combinatorial and Geometric Problems Related to Digital Halftoning," *Theoretical Foundations of Computer Vision: Geometry, Morphology, and Computational Imaging,* LNCS 2616, Springer, 2003.

[4] T. Asano, K. Obokata, N. Katoh, and T. Tokuyama: "Matrix rounding under the L_p-discrepancy measure and its application to digital halftoning," *Proc. ACM-SIAM Symposium on Discrete Algorithms*, pp. 896–904, San Francisco, 2002.

[5] B.E. Bayer: "An optimum method for two-level rendition of continuous-tone pictures," *Conference Record, IEEE International Conference on Communications,* 1, pp. (26-11)–(26-15), 1973.

[6] B. Chazelle: *The Discrepancy Method: Randomness and Complexity*, Cambridge University Press, 2000.

[7] D.E. Knuth, *The Art of Computer Programming.* volume 1, *Fundamental Algorithms*, 3rd ed. (Reading, Massachusetts: Addison-Wesley, 1997.

[8] Kodera Ed.: *Practical Design and Evaluation of Halftoned Images,* (in Japanese) Trikepps, 2000.

[9] J. Matoušek: *Geometric Discrepancy*, Springer, 1991.

研究業績一覧

学術論文

1. T. Shimamoto and T. Asano:
"Arranging Fewest Possible Probes to Detect a Hidden Object with Industrial Application", IEICE Trans. Fundamentals, 87-A (5), 1053-1058, 2004.
概要: This paper addresses the problem of arranging fewest possible probes to detect a hidden object in a specified region and presents a reasonable scheme for the purpose. Of special interest is the case where an object is a double-sided conic cylinder which represents the shape of the energy distribution of laser light used in the optical network. The performance of our scheme is evaluated by comparing the number of probes to that of an existing scheme, and our scheme shows a potential for reducing the number of probes. In other words, the time for detection is significantly reduced from a realistic point of view.

2. T. Asano, M. de Berg, O. Cheong, H. Everett, H. Haverkort, N. Katoh, and A. Wolff:
"Optimal Spanners for Axis-Aligned Buildings", Computational Geometry: Theory and Applications, 30, 1, 59-77, January 2005.
概要: The dilation of a geometric graph is the maximum, over all pairs of points in the graph, of the ratio of the Euclidean length of the shortest path between them in the graph and their Euclidean distance. We consider a generalized version of this notion, where the nodes of the graph are not points but axis-parallel rectangles in the plane. The arcs in the graph are horizontal or vertical segments connecting a pair of rectangles, and the distance measure we use is the L_1-distance. The dilation of a pair of points is then defined as the length of the shortest rectilinear path between them that stays within the union of the rectangles and the connecting segments, divided by their L_1-distance. The dilation of the graph is the maximum dilation over all pairs of points in the union of the rectangles. We study the following problem: Given n nonintersecting rectangles and a graph describing which pairs of rectangles are to be connected, we wish to place the connecting segments such that the dilation is minimized. We obtain four results on this problem: (i) for arbitrary graphs, the problem is NP-hard; (ii) for trees, we can solve the problem by linear programming on $O(n^2)$ variables and constraints; (iii) for paths, we can solve the problem in time $O(n^3 \log n)$; (iv) for buildings sorted vertically along a path, the problem can be solved in $O(n^2)$ time, and a $(1+\varepsilon)$-approximation can be computed in linear time.

3. T. Asano, D.G. Kirkpatrick, and C.K. Yap:
"Pseudo-approximation algorithm with applications to optimal motion planning", Discrete and Computational Geometry, 31, 1, 139-171, 2004.
概要: We introduce a technique for computing approximate solutions to optimization problems. If X is the set of feasible solutions, the standard goal of approximation algorithms is to compute $x \in X$ that is an ϵ-approximate solution in the following sense: $d(x) \leq (1+\epsilon)d(x^*)$ where $x^* \in X$ is an optimal solution, $d : X \to \mathcal{R}_{\geq 0}$ is the optimization function to be minimized, and $\epsilon > 0$ is an input parameter. Our approach is to first devise algorithms that compute pseudo ϵ-approximate solutions satisfying the bound $d(x) \leq d(x_R^*) + \epsilon R$ where $R > 0$ is a new input parameter. Here x_R^* denotes an optimal solution in the space X_R of R-constrained feasible solutions. The parameter R provides a stratification of X in the sense that (1) $X_R \subseteq X_{R'}$, for $R < R'$ and (2) $X_R = X$ for R suffi-

ciently large. We first describe a highly efficient scheme for converting a pseudo ϵ-approximation algorithm into a true ϵ-approximation algorithm. This scheme is useful because pseudo approximation algorithms seem to be easier to construct than ϵ-approximation algorithms. Another benefit is that our algorithm is automatically precision-sensitive. We apply our technique to two problems in robotics: (A) Euclidean Shortest Path (3ESP), namely the shortest path for a point robot amidst polyhedral obstacles in 3D, and (B) d_1-optimal motion for a rod moving amidst planar obstacles (1ORM). Previously, no polynomial time ϵ-approximation algorithm for (B) was known. For (A), our new solution is simpler than previous solutions and has an exponentially smaller complexity in terms of the input precision.

4. T. Asano, N. Katoh, H. Tamaki and T. Tokuyama:
"The structure and number of global roundings of a graph", Theoretical Computer Science, 325, 425-437, 2004.
概要: Given a connected weighted graph $G = (V, E)$, we consider a hypergraph $H_G = (V, \mathcal{P}_G)$ corresponding to the set of all shortest paths in G. For a given real assignment $\mathbf{a}$ on V satisfying $0 \leq \mathbf{a}(v) \leq 1$, a global rounding α with respect to H_G is a binary assignment satisfying that $|\sum_{v \in F} \mathbf{a}(v) - \alpha(v)| < 1$ for every $F \in \mathcal{P}_G$. We conjecture that there are at most $|V|+1$ global roundings for H_G, and also the set of global roundings is an affine independent set. We give several positive evidences for the conjecture.

研究会等

1. Boris Aronov, 浅野 哲夫, 菊地 洋右, Subhas C. Nandy, 笹原 慎司, 宇野 毅明:
"ディジタルハーフトーニングへの応用に向けての魔方陣の一般化 (1)", 情報処理学会アルゴリズム研究会, 100-9, 3 月，2005 年.
概要: 本論文では魔方陣を一般化した零 $k \times k$ discrepancy 行列を導入する．この行列は $n \times n$ 行列で，その要素は 0 から $n^2 - 1$ の整数値からなり，どの $k \times k$ 部分行列の値も一致する．まず，n と k に対して零 $k \times k$ discrepancy 行列が構成できるかが問題となる．本論文では零 $k \times k$ discrepancy 行列の存在の条件を述べる．特に $n = k^m$ である時，零 $k \times k$ discrepancy 行列の構成法について詳述する．このような零 $k \times k$ discrepancy 行列はディジタル・ハーフトーニングに用いられるディザ行列として良い性質を持つと考えられる．

2. Boris Aronov, 浅野 哲夫, 菊地 洋右, Subhas C. Nandy, 笹原 慎司, 宇野 毅明:
"ディジタルハーフトーニングへの応用に向けての魔方陣の一般化 (2)", 情報処理学会アルゴリズム研究会, 100-10, 3 月，2005 年.
概要: $n \times n$ の行列に整数 $0, \ldots, n^2 - 1$ を配置し，どの行和，列和も等しいものは準魔方陣と呼ばれる．ここでは列和，行和のかわりに $k \times k$ の部分行列に含まれる要素の和を考え，この和がすべて等しい $n \times n$ 行列を $k \times k$-ゼロディスクレパンシ行列とよぶ．本文では，このような行列が k と n がともに偶数であるとき存在し，k と n が互いに素であるとき存在しないことを示す．さらに，$k, m \geq 2$ を整数としたとき $n = k^m$ であるならば $k \times k$-ゼロディスクレパンシ行列の存在がいえる．この $k \times k$-ゼロディスクレパンシ行列の構成には定差行列が重要な役割を果たす．本文では，定差行列の特徴づけを行なう．

3. 浅野 哲夫, 崔 舜星, 橋間 信也, 菊地 洋右, 宋 少秋:
"正方行列上に一様に整数を配置する方法の提案とディジタルハーフトーニングへの応用", 情報処理学会アルゴリズム研究会, 100-12, 3 月，2005 年.
概要: 本論文では，$n \times n$ の正方行列上に 0 から $n^2 - 1$ までの整数をなるべく一様に配置する問題を考える．一様性を評価するため

にディスクレパンシに基づいた基準を導入する．すなわち，$k \times k$ の領域上での要素の和に注目し，その最大値と最小値の差をディスクレパンシとして定義する．n と k が共に偶数ならばディスクレパンシを 0 にする方法が知られている．本文では，n が奇数，$k = 2$ という基本的な場合について，ディスクレパンシを $2n$ にまで下げられることを示す．これは，従来の限界 $4n$ を改良したものになっている．数学のラテン方陣や魔方陣の理論で展開されている基本的な考え方をヒントとしている．この問題はディジタル・ハーフトーニングと密接な関係がある．低ディスクレパンシの行列を構成することができれば，オーダードディザ法の性能を向上できることが期待できる．

学会大会等

1. Xuefeng Liang and T. Asano:
"A Fast Denoising Method for Binary Fingerprint Image ", Proc. IASTED Conference on Visualization, Imaging, and Image Processing, No. 452-168, 309-313, September, 2004. In this paper we propose a fast method for binary fingerprint image denoising that employs the generalized and ordinary morphological operators based on Euclidian distance transform. This method avoids quite a number of computational redundance. In particular, the computations of denosing step are restricted to a minimum number of pixels. The results show that applying this method on fingerprint image with impulsive noise and useless components yields a segmentation much closer to that of an expect for extracting the minutia accurately.

2. Boris Aronov, Tetsuo Asano, Yosuke Kikuchi, Subhas C. Nandy, Shinji Sasahara, and Takeaki Uno:
"A Generalization of Magic Squares with Applications to Digital Halftoning", Proc. of 15th International Symposium on Algorithms and Computation, ISAAC 2004, Hong Kong, China, December 2004, 89-100, 2004. A semimagic square of order n is an $n \times n$ matrix containing the integers $0, \ldots, n^2 - 1$ arranged in such a way that each row and column add up to the same value. We generalize this notion to that of a zero $k \times k$-discrepancy matrix by replacing the requirement that the sum of each row and each column be the same by that of requiring that the sum of the entries in each $k \times k$ square contiguous submatrix be the same. We show that such matrices exist if k and n are both even, and do not if k and n are are relatively prime. Further, the existence is also guaranteed whenever $n = k^m$, for some integers $k, m \geq 2$. We present a space-efficient algorithm for constructing such a matrix. Another class that we call constant-gap matrices arises in this construction. We give a characterization of such matrices. An application to digital halftoning is also mentioned.

3. Xuefeng Liang, Arijit Bishnu, and Tetsuo Asano:
"A Near-Linear Time Algorithm for Binarization of Fingerprint Images Using Distance Transform", Proc. 10th International Workshop, IWCIA 2004, December, Auckland, Lecture Notes in Computer Science LNCS 3322, edited by R. Klette and J. Zunic, "Combinatorial Image Analysis,", 197-208, 197-208, 2004. Automatic Fingerprint Identification Systems (AFIS) have various applications to biometric authentication, forensic decision, and many other areas. Fingerprints are useful for biometric purposes because of their well known properties of distinctiveness and persistence over time. Fingerprint images are characterized by alternating spatial distribution of gray-level intensity values of ridges and ravines/valleys of almost equal width. Most of the fingerprint matching techniques re-

quire extraction of minutiae that are the terminations and bifurcations of the ridge lines in a fingerprint image. Crucial to this step, is either detecting ridges from the gray-level image or binarizing the image and then extracting the minutiae. In this work, we focus on binarization of fingerprint images using linear time euclidean distance transform algorithms. We exploit the property of almost equal widths of ridges and valleys for binarization. Computing the width of arbitrary shapes is a non-trivial task. So, we estimate width using distance transform and provide an time algorithm for binarization where M is the number of gray-level intensity values in the image and the image dimension is . With M for all purposes being a constant, the algorithm runs in near-linear time in the number of pixels in the image.

4. S. Sasahara, T. Asano:
"A new halftone technique to eliminate ambiguous pixels for stable printing", Proc Electronic Imaging Science and Technology, Color Imaging IX: Processing, Hardcopy, and Applications, 490-497, 2004. Digital halftoning is a technique to convert a continuous-tone image into a bi-level image. A cluster-dot halftoning reproducing continuous tone by changing the sizes of clusters has been commonly used in offset printing or xerography printers. Since a cluster consists of a number of small dots, fine control on the number of dots (cluster size) is required to reproduce a natural tone. Consequently, the cluster size becomes large, which degrades effective resolution. On the contrary, if we kept cluster size small to increase the effective resolution, then effective tone scale would be degraded. Thus, there is a tradeoff between effective resolution and effective tone scale. It was hard to balance these indices, especially in the case of low resolution printers. In this paper, we propose an algorithm which adaptively arranges or grows clusters according to spatial frequency of the cluster-dot halftoning by bubble packing to achieve a good balance between the two indices described above.

5. T. Asano, P. Brass, S. Sasahara:
"Disc Covering Problem with Application to Digital Halftoning", Proc. of the Workshop on Computational Geometry and Applications (CGA 04) as a part of International Conference on Computational Science and Its Applications – ICCSA 2004, Proceedings, Part III, pp.11-21, Assisi, Italy, 2004. Lecture Notes in Computer Science, LNCS 3045, part III, 3, 11-21, 2004 . This paper considers the following geometric optimization problem: Input is a matrix $R = (r_{ij})$. Each entry r_{ij} represents a radius of a disc with its center at (i, j) in the plane. We want to choose discs in such a way that the total area covered by exactly one disc is maximized. This problem is closely related to digital halftoning, a technique to convert a continuous-tone image into a binary image for printing. An exact algorithm is given for the one-dimensional version of the problem while approximation algorithms are given for the two-dimensional one. The approximation algorithms are verified to be satisfactory in practice through experiments in applications to digital halftoning.

6. Sachio Teramoto and T. Asano:
"Fast Implementation of Laguerre Voronoi Diagram with Hardware Assitance", Proc. International Symposium on Voronoi Diagrams in Science and Engineering, 165-171, September, 2004. In this paper we present a method for constructing Voronoi diagrams in Laguerre geometry (or power diagram) using graphics hardware. Advantages of the method are easiness of implementation and robustness over degeneracy. Efficiency of

this method is also shown by experimental results.

7. T. Asano, Naoki Katoh, Hisao Tamaki, and Takeshi Tokuyama:
"On Geometric Structure of Global Roundings for Graphs and Range Spaces", Proc. of the Scandinavian Workshop on Algorithm Theory (SWAT 04), 455-467, 2004. Given a connected weighted graph $G = (V, E)$, we consider a hypergraph $H_G = (V, \mathcal{P}_G)$ corresponding to the set of all shortest paths in G. For a given real assignment $\mathbf{a}$ on V satisfying $0 \leq \mathbf{a}(v) \leq 1$, a global rounding α with respect to H_G is a binary assignment satisfying that $|\sum_{v \in F} \mathbf{a}(v) - \alpha(v)| < 1$ for every $F \in \mathcal{P}_G$. We conjecture that there are at most $|V| + 1$ global roundings for H_G, and also the set of global roundings is an affine independent set. We give several positive evidences for the conjecture.

8. Boris Aronov, Tetsuo Asano, Naoki Katoh, Kurt Mehlhorn, and Takeshi Tokuyama:
"Polyline Fitting of Planar Points Under Min-sum Criteria", Proc. of 15th International Symposium on Algorithms and Computation, ISAAC 2004, Hong Kong, China, December 2004, also in Lecture Notes in Computer Science LNCS 3341, edited by R. Fleischer and G. Trippen, "Algorithms and Computation,", 77-88, 2004. Fitting a curve of a certain type to a given set of points in the plane is a basic problem in statistics and has numerous applications. We consider fitting a polyline with k joints under the min-sum criteria with respect to L_1- and L_2-metrics, which are more appropriate measures than uniform and Hausdorff metrics in statistical context. We present efficient algorithms for the 1-joint versions of the problem, and fully polynomial-time approximation schemes for the general k-joint versions.

C06: グラフ構造を有する問題に対する近似アルゴリズムの設計

永持 仁 † 　軽野 義行 ‡

† 京都大学 大学院 情報学研究科
〒 606-8501 京都市左京区吉田本町
nag@amp.i.kyoto-u.ac.jp

‡ 京都工芸繊維大学 工芸学部 機械システム工学科
〒 606-8585 京都市左京区松ヶ崎橋上町
karuno@kit.ac.jp

1 はじめに

通信網，電力網，交通網，VLSI の配線，スケジューリング問題，地理情報システム等の多くのシステム工学的，情報工学的諸問題に対するアルゴリズムを設計する場合には，これらを離散最適化問題として定式化することで，問題の持つ計算の複雑さの解明や高度な数学的解法の適用が可能となる．しかし，一般には，複雑な要求条件を含む現実の問題を離散最適化問題として定式化した場合には，分岐限定法や整数計画法といった離散最適化の汎用アルゴリズムしか適用できず，このままでは計算効率のよいアルゴリズムを得ることはできない．一方，遺伝アルゴリズム，シミュレーティッド・アニーリング法，タブーサーチ法などの計算の発見的手法に基づくソフトウエアも開発されているが，常に良質な答えを出力するという理論的な保証はなされていない．そこで，常に，最適解に対する近似の程度が理論的に抑えられているような答えを出力する，理論保障付き近似アルゴリズムの開発が望まれる．本研究では，グラフアルゴリズムを中心的な道具として，離散最適化問題に対する理論保証付きアルゴリズムの開発を行う．対象とする問題は，グラフの問題に限らず，グラフ論的手法の適用できる種々の問題を含む．

今年度までに得られた研究成果を以下の四つのカテゴリーに分類して報告する．

- グラフ連結度問題
- グラフの最小分割問題
- ミニマックス部分木被覆問題
- スケジューリング問題

2 グラフ連結度問題

グラフの連結度に関する問題に対しては研究代表者が１５年前に開発した最大隣接順序 (MA orderings) を利用した種々のアルゴリズムが設計されている．以下に述べる成果においても最大隣接順序によるグラフ疎化法 (sparsification) が重要な役割を果たしている．

グラフの点連結度　グラフの連結度を求めるアルゴリズムの研究はグラフアルゴリズムにおいても最も基本的な課題であり，その計算量は他の多くのグラフアルゴリズムの計算量に影響を与えている．グラフの枝連結度は比較的高速に計算することができるようになり，重み付きグラフの枝連結度 λ は $O(mn + n^2 \log n) = O(n^3)$ 時間で求められるようになっている．ここで，n, m はそれぞれグラフの点数，枝数である．これに対し，グラフの点連結度 κ を計算するには Gabow による現在最良のアルゴリズムを用いても $O(m + \min\{\kappa^{7/2}n, \kappa^2 n^{7/4}\})$ の計算時間がかかり，これは最悪 $\kappa = \Omega(n)$ のとき $O(n^{15/4})$ の計算量になることを意味する．そこで小さな計算量で点連結度を評価するアルゴリズムが開発されている．Henzinger は，グラフの最小次数を δ としたときに $\kappa \leq \delta$ の不等式が成立することを利用して，κ の 2 倍近似の値を求める $O(n^2 \min\{\kappa, \sqrt{n}\})$ 時間，$O(n^2)$ 領域のアルゴリズムを与えている．正確には，このアルゴリズムは $\kappa \leq \lfloor \delta/2 \rfloor$ の場合に正しい κ の値を出力し，そうでない場合には $\kappa > \lfloor \delta/2 \rfloor$ というメッセージを出力する．Gabow は，固定された値 $\alpha < 1$ に対して $\kappa \leq \alpha\delta$ のとき最小点カット（点連結度を達成している点カット）を出力し，そうでない場合は $\kappa > \alpha\delta$ というメッセージを出

力する $O(\kappa^2 n^{3/2} + \kappa n^2)$ 時間，$O(m)$ 領域のアルゴリズムを与えている．

本研究では，最大隣接順序によるグラフ疎化法を Henzinger のアルゴリズムに適用することにより計算時間，計算領域を縮めることに成功した．我々のアルゴリズムは $O(n^2(1 + \min\{\kappa^2, \kappa\sqrt{n}\}/\delta))$ 時間，$O(n + m)$ 領域の計算量で，$\kappa \leq \lfloor \delta/2 \rfloor$ の場合に最小点カット（点連結度を達成している点カット）を出力し，そうでない場合は $\kappa > \lfloor \delta/2 \rfloor$ というメッセージを出力する．提案するアルゴリズムは δ が κ と比べて大きい場合には従来よりも高い性能を発揮する．

最小 (s,t)-カット　グラフにソース，シンクと呼ぶ 2 点 s，t が与えられたとき，ソースシンク間の最大 (s,t)-フローあるいは最小 (s,t)-カットは，グラフアルゴリズムの理論的な観点のみならず，広範囲な用途を持つことからもこれらを計算する高速なアルゴリズムの開発は非常に重要な研究課題である．過去２０年にわたって最大フローアルゴリズムの開発が続き，大きな成果をもたらしている．しかし，枝の容量が 1 である場合の最大流問題はグラフの辺素なパス集合を求める問題であり，この場合に対してさらに高速に作動するアルゴリズムの開発が行われている．この単位容量の場合には，有向グラフに対する Dinits のアルゴリズムの計算時間は $O(\min\{\nu, n^{2/3}, m^{1/2}\}m)$ である（ここで ν は最大流の値である）．その後，有向グラフに対しては研究の進展がないが，Goldberg と Rao は，グラフが単位容量でありかつ無向であれば Dinits のアルゴリズムにおいて各ブロックフローを計算した残余ネットワークに対して最大隣接順序 (MA orderings) によるグラフ疎化法を適用することで計算量を $O(\min\{m, n^{3/2}\}m^{1/2})$ に減らすことができることを示した．Karger と Levine はグラフ疎化法をさらに巧妙に用いて $O(m + \nu^{3/2}n)$ 時間のアルゴリズムと $O(\nu^{1/6}nm^{2/3})$ 時間のアルゴリズムを得ている．しかし，有向グラフに対して直接有効なグラフ疎化法は現在知られておらず，有向グラフに対する最大フロー，最小カットの計算時間を改善することは未解決問題である．本研究では，有向グラフに対し，無向グラフへの「近さ」を表す尺度を導入し，無向グラフに近い有向グラフに対しては無向グラフに対するグラフ疎化法を用いた高速最大流アルゴリズムが適用できることを示した．有向グラフ $D = (V, E)$ の無向グラフへの近さの指標 μ は $\sum_{u \in V - \{s,t\}}$(点 u に入る枝数−点 u から出る枝数) で定義される．このとき提案するアルゴリズムは有向グラフ D の最小 (s,t)-カットを $O(\min\{m + \nu(\nu+\mu)^{1/2}n,\ (\nu+\mu)^{1/6}nm^{2/3}\})$ 時間で計算する．この計算量は小さな μ を持ちかつ密であるような有向グラフに対しては従来法よりも優れた性能を発揮する．

グラフの局所２点連結増大問題　グラフの連結度増大問題 (graph augmentation problem) とは，与えられたグラフにいくつかの辺を新たに加えることでその辺連結度あるいは点連結度を指定された目標の値に増大させる問題であり，このとき加える辺の本数を最小にすることが目的となる．この問題は，信頼性ネットワーク設計問題，フロアプランにおける矩形双対問題，フレームの剛体問題，データセキュリティ問題，グラフ描画問題等に応用を持つ．グラフの連結度増大問題は 1976 年の Eswaran と Tarjan の論文によって最初に論じられ，この論文ですでにグラフの 2-辺連結化あるいは 2-点連結化問題，および有向グラフの強連結化問題が多項式時間で解けることが示されている．任意の正整数 k に対してグラフの k-辺連結化問題が多項式時間で解けることを初めて示したのは atanabe と Nakamura である．現在この問題は，辺連結度を求めるのとほぼ同程度の計算時間で解けることが Nagamochi と Ibaraki により示されている．一方，点連結度を局所的に増大させる問題はＮＰ困難問題であることが示されている．本研究では局所２点連結化問題に対して 4/3-近似アルゴリズムが設計できることを示した．与えられた単純連結グラフ $G = (V, E)$ および 2 点対の集合 R に対して，何本かの新しい枝をグラフ G に付与して R の各 2 点対間の局所点連結度を 2 以上にする問題を考える．このとき加える枝の本数を最小にすることが目的である．この問題に対しては 3/2-近似アルゴリズムが知られていたが本研究では問題に対する下界の導き方を精密化することで最適な付加枝集合の大きさの高々4/3 倍の解を求める線形時間アルゴリズムの設計に成功した．

3　グラフの最小分割問題

正整数 k が与えられ，グラフの節点集合を k 個の部分集合に分割したとき，異なる部分集合間にまたがる辺の集合を k-分割カット (k-way cut, k-cut) と呼ぶ．目的関数は，k-分割カットに含まれる辺の本数，あるいは，辺に重みが付与されている場合には，k-分割カット内の辺の重み和とし，これを最小にすることが問題の目的である．最小 k-分割を求める問題は，VLSI の設計，ページメモリ問題，系統樹問題並列処理におけるタスク割付問題，巡回セールスマン問題の解法，グラフの強度計算，ネットワーク信頼性解析などにおいて重要な応用を持つ．

一般に 2^V を定義域とする実数値関数 f を V 上の集合関数といい，f が次の不等式を満足するとき劣モジュラ (submodular) と呼ばれる．

$$f(X)+f(Y) \geq f(X \cap Y)+f(X \cup Y), \quad \forall X, Y \subseteq V.$$

また，任意の $S \subseteq V$ に対し $f(S) = f(V-S)$ を満たすとき f は対称 (symmetric) であると言う．f を V 上の劣モジュラ集合関数としたとき，(V, f) を劣モジュラシステムといい，

$$cost_f(\pi) = f(V_1) + f(V_2) + \cdots + f(V_k)$$

を最小にする V の k-分割 π を求める問題を劣モジュラシステム上の k-分割問題 (the k-partition problem in submodular systems) と呼び k-PPSS と略す．特に，f が対称劣モジュラである場合には，対称劣モジュラシステム上の k-分割問題 (the k-partition problem in symmetric submodular systems) と呼び k-PPSSS と略す．明らかに問題のクラスの包含関係として k-PPG $\subset$ k-PPH $\subset$ k-PPSSS $\subset$ k-PPSS が成り立つ．ただし，k-PPSSS, k-PPSS について問題を解く計算の手間には，通常の基本演算以外に，指定された $S \subseteq V$ に対する $f(S)$ の値を評価する手続き（オラクル）の手間が含まれる．以下では，$f(S)$ の値を得るためにかかる手間を θ と書くことにする．f 値を評価するオラクルを呼び出す回数が多項式回であるようなアルゴリズムをオラクル多項式アルゴリズムと呼ぶ．

グラフのカットに関する問題を解く上で重要な道具は最大流アルゴリズムである．有向グラフ上でソース s とシンク t の 2 節点が指定されたとき，s から t への有向パスをなくすために取り除くべき辺集合の最小の重み和は，s から t への流れの最大値に等しいことが最大流最小カットの定理として知られている．この s から t への最大流と s と t を分離するカットは多項式時間で求めることができる．この計算量を $F(n, m)$ で表す．現在，$F(n, m) = O(mn \log(n^2/m))$ が知られている．従って，無向グラフの最小 2-端子カットを $F(n, m)$ 時間で求めることができる．

グラフの最小 2-端子カット問題は最大流アルゴリズムを 1 回使えば解くことができる．グラフの最小カットを計算する問題 2-PPG は，$V = \{v_1, v_2, \ldots, v_n\}$ としたとき，最小 2-端子カット問題を二つの端子 s, t を $s = v_1, t \in \{v_2, v_3, \ldots, v_n\}$ の $n-1$ 通りに対して解き，その中の費用最小のカットを出力することで解くことができる．Hao と Orilin は最大流アルゴリズムを 1 回適用する間に，2-PPG を解くための情報を取り出すことで 2-PPG を解く計算時間を $O(nm \log(n^2/m))$ に減らした．Nagamochi と Ibaraki は最大隣接順序と呼ばれる別の手続きを利用して 2-PPG に対する $O(mn + n^2 \log n)$ 時間アルゴリズムを与えた．重みの重い辺ほど「その辺は最小 2-分割カットには使われない」と高い確率で判断し，その辺を縮約してグラフを小さくしていくというアイディアに基づき，Karger や Karger と Stein はそれぞれ，2-PPG に対する $\tilde{O}(n^2)$ 時間，$\tilde{O}(m)$ 時間のモンテカルロ型確率アルゴリズムを与えた（$\tilde{O}$ は対数多項式 $\log^c n$ を省略した表記である）．一般の k に対し，k-PPG は，分割数 k を入力変数とみると NP-困難な問題になることが Goldschmidt と Hochbaum により示された（よって，k, n, m の多項式時間で k-PPG を解くことは望めない）．Karger と Stein は，確率的縮約の考え方を使い，k-PPG に対する $O(n^{2(k-1)}(\log n)^3)$ 時間モンテカルロ型確率アルゴリズムを与えた．

$C_k(n, m)$ を k-PPG を決定性アルゴリズムにより解く計算量の上界とする．Goldschmidt と Hochbaum は k を固定したときには k-PPG が多項式時間で解けることを示した．この計算量は，$C_k(n, m) = O(n^{k^2/2-3k/2+4} F(n, m))$ であり，一般の k に対しては現在最良の結果である．このアルゴリズムのおおまかなアイディアは以下の通

りである．与えられたグラフの最小 k-分割カットを $\pi_k^* = \{V_1^*, V_2^*, \ldots, V_k^*\}$ とする．ただし，添え字は $cut_G(V_1^*) \leq cut_G(V_2^*) \leq \cdots \leq cut_G(V_k^*)$ を満たすとする．まず，最小 k-分割カット $\pi_k^* = \{V_1^*, V_2^*, \ldots, V_k^*\}$ の最初のカット V_1^* を見つけ，そこを固定する（すなわちグラフから V_1^* を除く）ことで問題を $G[V - V^*]$ 上の $(k-1)$-PPG に帰着させる．そのような V_1^* を特定することは難しいが，いくつか 2-分割カット $\{X, V - X\}$ を選び出しし，その中に $\{V_1^*, V - V_1^*\}$ が含まれるようにするのは可能である．Goldschmidt と Hochbaum は，必ず V_1^* を拾い上げることのできる $O(n^k)$ 個の 2-分割カットの選び方を見つけ，k-PPG を $O(n^k)$ 個の $(k-1)$-PPG に帰着できることを示した．

分割数 k が小さい場合には，問題の構造が詳しく調べられ，帰着に必要な 2-分割カットの数を減らすことで計算時間が改善されている．3-PPG に対する計算量 $C_3(n, m)$ としては，Kapoor，Kamidoi らよる $O(n^3 F(n, m)) = \tilde{O}(mn^4)$，Burlet と Goldschmidt による $\tilde{O}(mn^3)$ が知られている．4-PPG に対しては，Kapoor，Kamidoi らによる $O(n^4 F(n, m)) = \tilde{O}(mn^5)$ が知られている．最近，$k \in \{3, 4, 5, 6\}$ に対して，Nagamochi らによる $C_k(n, m) = O(mn^k \log(n^2/m))$ が示された．この方法に確率的縮約を組合せることで Levine は $k \in \{3, 4, 5, 6\}$ に対し $O(mn^{k-2} \log^3 n)$ 時間のモンテカルロ型確率アルゴリズムを与えた．

以下では分割数 k に関しても多項式時間で作動するような最小 k-分割カット問題に対する近似アルゴリズムについて紹介する．

k-PPG の最適解の $(2 - \frac{2}{k})$ 倍以内の近似解を与える簡便な方法が Saran と Vazirani や Kapoor により与えられている．この方法では，1-分割 V (つまり，全体の点集合) から始め，分割数を一つ増やすような最小費用の 2-分割カットを計算し，これを繰り返すことで k-カットを構成する．得られた k-カットは最小とは限らないが，最適解の高々 $(2 - \frac{2}{k})$ 倍以内であることが証明されている．また，このアルゴリズムは対称劣モジュラシステムに対しても作動するように拡張でき，k-PPSSS についても同様に $(2 - \frac{2}{k})$ 倍近似の性能が得られることが Queyranne により指摘されている．しかし，以上のアルゴリズムの正当性に関する証明は Gomory-Hu 木の構造に頼った複雑なものであり，カット関数の一般化である劣モジュラ集合関数においてはもはや Gomory-Hu 木型の構造が得られないことも知られている．

本研究では最小 2-分割の追加による k-分割の生成アルゴリズムの簡潔な正当性の証明を示し，これに基づき劣モジュラ集合関数への一般化を行った．さらに，このアルゴリズムの近似性能を改善するために，最小 2-分割ではなく，最小 3-分割を計算しながら分割数を二つずつ増やすアルゴリズムについて研究した（$k \geq 4$ が偶数のときは 1 回目のみ最小 2-分割で分割数を一つだけ増やす）．彼らはこのアルゴリズムの近似性能が $(2 - \frac{3}{k})$（k が奇数のとき），$(2 - \frac{3k-4}{k^2-k})$（k が偶数のとき）であることを証明した．グラフの最小 k-分割カットの多項式近似としてはこれが現在最良である．

さらに，本研究では，与えられた劣モジュラシステム (V, f) に対し，最小 2-分割を計算しながら分割数を k にまで増やすアルゴリズムを貪欲分離アルゴリズム (Greedy Splitting Algorithm，以下 GSA と略す) を提案し，その近似性能について解析を行った．このアルゴリズム GSA は $k-1$ 回反復を行い，第 i 回目の反復では V の $(i+1)$-分割 π_{i+1} を構築する．まず $\pi_1 = \{V\}$ と初期設定し，その後，π_i の一つの部分集合 $W \in \pi_i$ を最小費用で分割することで $(i+1)$-分割 π_{i+1} を得る．正確には，$f(S) + f(W - S) - f(W)$ (π_i から π_{i+1} を得るための費用の増加分) を最小にするような $W \in \pi_i$ とその 2-分割 $\{S, W - S\}$ を計算する．この最小 2-分割を $\{S_i, W_i - S_i\}$ と書くと，$(i+1)$-分割 π_{i+1} は，π_i において W_i を S_i と $W_i - S_i$ に入れ替えることで得られる．従って，各 $\ell = 1, 2, \ldots, k$ に対し $cost_f(\pi_\ell) = f(V) + \sum_{i=1}^{\ell-1} (f(S_i) + f(W_i - S_i) - f(W_i))$ が成り立つ．明らかに π_k は V の k-分割である．各 $W \in \pi_i$ に対し $f(S) + f(W - S) - f(W)$ を最小にする W の空でない真部分集合 S を $O(|W|^3\theta)$ 時間で見つけることができるので GSA の計算量は $\sum_{W \in \pi_i} O(|W|^3\theta) = O(|V|^3\theta)$ となる．

V 上の集合関数 f に対し，α_f を V の任意の k-分割 $\{V_1, \ldots, V_k\}$ に対して $\sum_{i=1}^k f(V - V_i) \leq \alpha \sum_{i=1}^k f(V_i)$ を満す最小の数 α とする．

このとき，非負劣モジュラシステム (V, f) に対し GSA は最適解の $(1 + \alpha_f)(1 - \frac{1}{k})$ 倍以内の V の k-分割を出力することを証明することができる．

対称な劣モジュラ集合関数 f に対しては $\alpha_f \leq 1$ であるので，従来から知られていた Saran と Vazirani，Kapoor による k-PPG に対する結果や Queyranne による k-PPSSS に対する結果は，本研究で得られた結果の系として得られる．また，一般の劣モジュラシステム (V, f) の任意の k-分割 $\{V_1, \ldots, V_k\}$ に対し，$\sum_{i=1}^{k} f(V - V_i) \leq (k-1)\sum_{i=1}^{k} f(V_i) - k(k-2)f(\emptyset)$ が成り立つ．さらに，非負劣モジュラシステムでは $f(\emptyset) \geq 0$ より，$\alpha_f \leq k-1$ であるので k-PPSS は $(k-1)$ 倍近似可能である．

4　ミニマックス部分木被覆問題

複数台の配送車両が与えられた搬送経路ネットワーク上の配送業務を分担して処理する際に，車両に与えられる最大の負荷を最小にする問題を考え，グラフ理論的なアプローチを行う．まず，搬送経路ネットワークを各枝と点に非負重みを持つ連結グラフ $G = (V, E)$ によりモデル化する．枝 $e \in E$ および点 $v \in V$ の重みをそれぞれ $w(e)$, $h(v)$ と表す．ここで $w(e)$ は枝 e を通過するときの移動コスト（移動時間）を意味し，$h(v)$ は点において行う作業に対するコスト（作業時間）を表す．デポの役割をする点を r とし，車両台数を表す整数を p とする．このとき，ミニマックス部分木カバー問題 (the minmax subtree cover problem: MSC) とは，点集合 V の p 分割 $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ と p 個の部分木 $T_1, T_2, \ldots, T_p$（ただし，各 T_i は $X_i \subseteq V(T_i)$ を満たすもの）を実行可能解とし，部分木の最大コストを最小にすることを目的関数とする．ここで，部分木 T_i のコストは T_i の枝の重み和と X_i の点の重み和の合計として定義される．この問題にデポを考慮することで定義されるミニマックス根付き部分木カバー問題 (the minmax rooted-subtree cover problem: MRSC) とは，点集合 V の p 分割 $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ と p 個の部分木 $T_1, T_2, \ldots, T_p$（ただし，各 T_i は $X_i \cup \{r\} \subseteq V(T_i)$ を満たすもの）を実行可能解とし，部分木の最大コストを最小にすることを目的関数とする．さらに，ミニマックス根付き閉路カバー問題 (the minmax rooted-cycle cover problem: MRCC) とは，点集合 V の p 分割 $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ と p 個のサイクル $C_1, C_2, \ldots, C_p$（ただし，各 C_i は $X_i \cup \{r\} \subseteq V(C_i)$ を満たすもの）を実行可能解とし，サイクルの最大コストを最小にすることを目的関数とする．以上の問題は枝重みに三角不等式が成立している場合や G が木に限定されている場合でもＮＰ困難であることが示されている．以下，n，m をそれぞれ与えられたグラフ G の点の数，枝の数とする．

本研究ではまず与えられたグラフ G が木である場合に対して近似アルゴリズムを設計した．MSC に対しては従来，$O(p^{p-1}n^{p-1})$ 時間の $(2 - \frac{2}{p+1})$ 近似アルゴリズムが知られていたが，分割すべき点の集合を木 G の節点部分集合に変更できるよう拡張した上で，問題の $(2 - \frac{2}{p+1})$ 近似解を求めるアルゴリズムの計算量を $O((p-1)! \cdot n)$ に軽減した．この計算量は p に関しては指数的であるが固定された p に対しては線形時間である．木 G に対する MSC に対しては，さらに木に対する点分割のアルゴリズムを利用することで $(2 - \frac{2}{p+1})$ 近似解を求める $O(p^2 n)$ 時間のアルゴリズムを設計した．ここでは枝集合分割問題を点集合分割問題へ変換する方法を新たに開発した点が特徴である．

次に木 G に対する MRSC に対しては，木 G に対する MSC に対する上記の結果を用いた 3 倍近似の線形時間アルゴリズムをまず設計し，これに基づきさらに近似精度の高い $(2+\varepsilon)$ 近似解を構築する $O(n \log \frac{1}{\varepsilon})$ 時間アルゴリズムを設計した（ε はパラメータとして入力される整数である）．

本研究では G が一般の連結グラフである場合の MRSC に対して $O(m + n \log n)$ 時間の $(3 - 2/(p+1))$ 近似アルゴリズムが構築できることを示した．この結果に基づきグラフ G の枝重みが三角不等式を満たす場合には MRCC に対する $(6 - 4/(p+1))$ 近似アルゴリズムが設計できることを証明した．以上の結果は後述する配送スケジューリングにおける近似アルゴリズムの設計において重要な役割を果たしている．

5　スケジューリング問題

本研究課題内のこの研究テーマにおいては，スケジューリング問題に対する近似アルゴリズムの設計を検討している．扱うのは，大きく分けて，搬送スケジューリングと機械スケジューリングの二種類である．特に，配送スケジューリングの問

題では，ジョブの処理をおこなうビークルが，走行経路を表すグラフの上を移動する．よって，そのグラフの構造を考慮に入れたアルゴリズムを設計することによって，優れた近似比を実現できる可能性が大きい．

5.1 配送スケジューリング

本年度は，まず，木構造グラフにおける配送スケジューリング問題，および，部分木被覆問題に対する過去の研究の整理をおこなった．搬送スケジューリング問題では，複数台のビークルが，走行経路として与えられたグラフの上を移動しながら，節点上に存在するジョブの処理をおこなう．問題の目的は，与えられた目的関数を最小（あるいは最大）にするような各ビークルの担当ジョブ，および，その割り当てられたジョブの処理順序を決定することである．代表的な目的関数は，ジョブの完了時刻の関数であるメイクスパン，ツアータイム，最大納期ずれなどである．なお，特別な場合として，一台のビークルのスケジューリングを扱うこともある．一方，部分木被覆問題とは，与えられたグラフをいくつかの部分木に分割する問題である．グラフの枝と節点には，非負の重みが与えられており，代表的な目的関数は，各部分木のコスト（その枝の重みと節点の重みの総和）の最大値の最小化である．

この整理の作業は，各ビークルの担当ジョブ（が置かれている節点の集合）に誘導される部分グラフを，ある部分木で近似できないかという考えに動機づけられている．部分木被覆問題における枝の重みを，配送スケジューリング問題におけるビークルの移動時間，また，節点の重みをビークルがジョブを処理するための時間とみなせば，二つの問題には似ている点が多い．実際，この整理の作業の過程で，与えられたグラフが木の場合の部分木被覆問題に対する定数倍近似アルゴリズムをサブルーチンとして用いることによって，メイクスパン最小化を目的とした木構造グラフにおける配送スケジューリング問題に対して，5 倍近似アルゴリズム（デポが指定されている場合は 3 倍近似アルゴリズム）を構成できることを示した．

次に，配送に使用するビークルの台数最小化問題を検討するための準備として，部分木数最小化を目的とした部分木被覆問題を取り上げた．台数という目的関数はジョブの完了時刻の直接的な関数ではないので，配送スケジューリング問題の研究において，これを扱った例は過去にあまり無いようである．この研究テーマでの成果は，与えられたグラフが木の場合の部分木数最小化を目的とした部分木被覆問題に対して，最大コスト最小化部分木被覆問題に対する定数倍近似アルゴリズムをサブルーチンとして用いることによって，一つの下界値と多項式的な計算手間で動作する 3 倍近似アルゴリズムを与えたことである．配送スケジューリング問題の立場からすると，台数が最適値の 3 倍であるということは，実用的にはまだ十分な近似性能であるとは言えないかも知れない．しかしながら，ジョブの完了時刻の関数ではない目的関数に対して，このような定数倍近似アルゴリズムが存在することを示したのは新しい知見である．

以上が，本年度における配送スケジューリング問題に対する研究の進展状況である．本年度の研究成果から，部分木被覆問題に対する高性能な近似アルゴリズムが得られれば，関連する配送スケジューリング問題に対する有用な近似アルゴリズムを構成できる可能性も大きくなることが予想される．それを踏まえて，今後もこの方面からアプローチしていく予定である．

5.2 機械スケジューリング

機械スケジューリング問題の分類のやり方として，与えられる機械台数によって分ける，つまり，一機械スケジューリング問題と多機械スケジューリング問題とに分ける方法がある．このとき，多機械問題は，さらに，並列機械問題とショップ問題とに分けられる．並列機械問題では，処理されるべき各ジョブは，複数ある機械のいずれか一台において処理を受ければよい．一方，ショップ問題では，各ジョブがいくつかの機械を渡り歩いてその処理が完了する．代表的なショップモデルとして，ジョブショップ問題，フローショップ問題，オープンショップ問題などがある．

グラフ構造は，例えば，ジョブショップスケジューリング問題におけるジョブの移動経路の表示に現れる．ジョブショップ問題では，各ジョブご

とにそれぞれの移動経路が定められており，その情報を含む隣接グラフという有向グラフがしばしば利用される．

ジョブショップ問題において，すべてのジョブの移動経路が同一であるとき，その問題は，特別に，フローショップ問題と呼ばれる．この研究テーマで扱うショップ問題の一つに，タイムラグを考慮した 2 機械フローショップ問題がある．この問題に対しては，n をジョブ数としたとき，$O(n \log n)$ 時間で動作する 2 倍近似アルゴリズムと多項式時間近似スキーム（以下，PTAS と略記）が存在することが示されていたが,（それぞれ M. Dell'Amico, *Operations Research*, 44 (1996) 777–787，L. A. Hall, *Mathematical Programming*, 82 (1998) 175–190）．後に我々も $O(n \log n)$ 時間で動作する 11/6 倍近似アルゴリズムを与えた．

今の時点で，理論的な近似精度の観点からは PTAS が最も優れているが，計算手間や実装の容易性といった観点からはまだ検討しなければならないことがいくつか残っている．

6　おわりに

今年度の研究成果は主に，連結度問題に対する近似アルゴリズムの開発，グラフ分割問題に対する近似アルゴリズムの開発，ミニマックス部分木問題に対する近似アルゴリズムの開発，スケジューリング問題に対する近似アルゴリズムの開発であった．これらの問題はそれぞれの定式化は異なっているが互いに関連性を持っているように思われる．特に，グラフ分割問題とミニマックス部分木問題は最適化すべき目的関数は異なるが最適化すべき方向性は類似しているので，これらの問題を統一的に扱えるような近似アルゴリズムの設計手法が確立できれば有用であると考えられる．これまでに用いたアルゴリズムの設計手法を整理してグラフ構造を持つ広範囲の問題が扱えるように今後も一般化を目指していく．

研究業績一覧

学術論文

1. H. Nagamochi, K. Suzuki, T. Ishii:
   “A Simple Recognition of Maximal Planar Graphs”, Information Processing Letters, 89, 223-226, 2004.
   概要: In this paper, we propose a linear time algorithm for checking whether a given graph is a maximal planar graph or not and for delivering a planar embedding if it is so. Our algorithm is based on a canonical ordering, which was first introduced by de Fraysseix et al. to draw a maximal planar graph in the plane so that each edge is depicted by a straight line segment. We show that an algorithm for computing a canonical ordering can be used to test whether or not an arbitrarily given graph is a maximal planar graph. Our algorithm needs no sophisticated data structure and considerably easy to implement.

2. H. Nagamochi, K. Okada:
   “A Faster 2-Approximation Algorithm for the Minmax p–Traveling Salesmen Problem on a Tree”, Discrete Applied Mathematics, 140, 103-114, 2004.
   概要: Given an edge-weighted tree T and an integer $p \geq 1$, the minmax p–traveling salesmen problem on a tree T asks to find p tours such that the union of the p tours covers all the vertices. The objective is to minimize the maximum of length of the p tours. It is known that the problem is NP-hard and has a $(2 - \frac{2}{p+1})$-approximation algorithm which runs in $O(p^{p-1}n^{p-1})$ time for a tree with n vertices. In this paper, we consider an extension of the problem in which the set of vertices to be covered now can be chosen as a subset S of vertices and weights to process vertices in S are also introduced in the tour length. For the problem, we give an approximation algorithm that enjoys the same ap-

proximation ratio, but runs in $O((p-1)! \cdot n)$ time.

3. H. Nagamochi, N. Yamada:
"Counting Edge Crossings in a 2-Layered Drawing", Information Processing Letters, 91, 221-225, 2004.
概要: Given a bipartite graph $G = (V, W, E)$ with a bipartition $\{V, W\}$ of a vertex set and an edge set E, a 2-layered drawing of G in the plane means that the vertices of V and W are respectively drawn as distinct points on two parallel lines and the edges as straight line segments. We consider the problem of counting the number of edge crossings. In this paper, we design two algorithms to this problem based on the dynamic programming and divide-and-conquer approaches. These algorithms run in $O(n_1 n_2)$ time and $O(m)$ space and in $O(\min\{n_1 n_2, |E| \log(\min\{|V|, |W|\})\})$ time and $O(m)$ space, respectively. Our algorithms outperform the previously fastest $\Theta(|E| \log(\min\{|V|, |W|\}))$ time algorithm for dense graphs.

4. L. Zhao, H. Nagamochi, T. Ibaraki:
"On Generalized Greedy Splitting Algorithms for multiway partition problems", Discrete Applied Mathematics, 143, 130-143, 2004.
概要: Given a system (V, T, f, k), where V is a finite set, $T \subseteq V$, $f : 2^V \to \mathbf{R}$ is a submodular function and $k \geq 2$ is an integer, the general *multiway partition problem* (MPP) asks to find a k-partition $\mathcal{P} = \{V_1, V_2, \ldots, V_k\}$ of V that satisfies $V_i \cap T \neq \emptyset$ for all i and minimizes $f(V_1) + f(V_2) + \cdots + f(V_k)$, where $\mathcal{P}$ is a k-partition of V if (i) $V_i \neq \emptyset$, (ii) $V_i \cap V_j = \emptyset$ $(i \neq j)$, and (iii) $V_1 \cup V_2 \cup \cdots \cup V_k = V$ hold. MPP formulation captures a generalization in submodular systems of many NP-hard problems. Previously, the authors gave a simple framework for approximating MPP problems by greedily increasing the size of partition one by one. In this paper, we show that improved factors are available by increasing the size by two. We also provide polynomial time implementations for some MPP problems. Our approach, however, does not help for the variant of increasing the size by three (or more).

5. H. Nagamochi:
"Graph Algorithms for Network Connectivity Problems", J. Operations Research Society of Japan, 47, 199-223, 2004.
概要: This paper surveys the recent progress on the graph algorithms for solving network connectivity problems such as the extreme set problem, the cactus representation problem, the edge-connectivity augmentation problem and the source location problem. In particular, we show that efficient algorithms for these problems can be designed based on maximum adjacency orderings.

6. H. Nagamochi:
"On 2-Approximation to the Vertex-Connectivity in Graphs", Inst. Electron. Inform. Comm. Eng. Trans. Information and Systems, E88-D, 12-16, 2005.
概要: Given a graph G, we give a fast algorithm for approximating the vertex connectivity κ of G. Our algorithm delivers a minimum vertex cut of G if $\kappa \leq \lfloor \delta/2 \rfloor$, and returns a message "$\kappa > \lfloor \delta/2 \rfloor$" otherwise, where δ denotes the minimum degree of G. The algorithm runs in $O(n^2(1 + \min\{\kappa^2, \kappa\sqrt{n}\}/\delta))$ time and $O(n+m)$ space, where n and m denote the numbers of vertices and edges in G, respectively.

7. L. Zhao, H. Nagamochi, T. Ibaraki:
"A Greedy Splitting Algorithm for Approximating Multiway Partition Problems", Mathematical Programming, 102, 167-183, 2005.
概要: Given a system (V, T, f, k), where V

is a finite set, $T \subseteq V$, $f : 2^V \to \mathbf{R}$ is a submodular function and $k \geq 1$ is an integer, the general *multiway partition problem* (MPP) asks to find a k-partition $\mathcal{P} = \{V_1, V_2, \ldots, V_k\}$ of V that satisfies $V_i \cap T \neq \emptyset$ for all i and minimizes $f(V_1) + f(V_2) + \cdots + f(V_k)$, where $\mathcal{P}$ is a k-partition of V if (i) $V_i \neq \emptyset$, (ii) $V_i \cap V_j = \emptyset$ $(i \neq j)$, and (iii) $V_1 \cup V_2 \cup \cdots \cup V_k = V$ hold. MPP includes NP-hard problems *k-way cut*, *multiterminal cut*, *target split* and their generalizations in hypergraphs. We present a simple and unified framework for developing and analyzing approximation algorithms for MPPs. It starts at $\{V\}$ and greedily increases the size of partition by one in each of $k-1$ iterations. We prove some interesting properties and derive performance guarantees for many MPPs.

8. H. Nagamochi:
"On Computing Minimum (s,t)-Cuts in Digraphs", Information Processing Letters, 93, 231-237, 2005.
概要: Let $D = (V, E)$ be a simple digraph with n vertices and m edges, and s and t be vertices designated as a source and a sink. The currently fastest algorithm that computes a minimum (s,t)-cut in D runs in $O(\min\{\nu, n^{2/3}, m^{1/2}\}m)$ time, where ν is the size of a minimum (s,t)-cut. In this paper, we define the non-eulerianness μ as the sum of $|\#\text{incoming edges at } u - \#\text{outgoing edges at } u|$ over all $u \in V - \{s,t\}$, and prove that a minimum (s,t)-cut in D can be obtained in $O(\min\{m + \nu(\nu+\mu)^{1/2}n,\ (\nu+\mu)^{1/6}nm^{2/3}\})$ time. This outperforms the previous algorithm when D is a dense digraph with small μ.

9. H. Nagamochi:
"On the One-Sided Crossing Minimization in a Bipartite Graph with Large Degrees", Theoretical Computer Science, 332, 417-4467, 2005.
概要: Given a bipartite graph $G = (V, W, E)$, a 2-layered drawing consists of placing nodes in the first node set V on a straight line L_1 and placing nodes in the second node set W on a parallel line L_2. For a given ordering of nodes in W on L_2, the one-sided crossing minimization problem asks to find an ordering of nodes in V on L_1 so that the number of arc crossings is minimized. A well known lower bound LB on the minimum number of crossings is obtained by summing up $\min\{c_{uv}, c_{vu}\}$ over all node pairs $u, v \in V$, where c_{uv} denotes the number of crossings generated by arcs incident to u and v when u precedes v in an ordering. In this paper, we prove that there always exits a solution whose crossing number is at most $(1.2964 + 12/(\delta - 4))LB$ if the minimum degree δ of a node in V is at least 5.

10. H. Nagamochi:
"An Improved Bound on the One-Sided Minimum Crossing Number in Two-Layered Drawings", Discrete and Computational Geometry, (掲載予定).
概 要: Given a bipartite graph $G = (V, W, E)$, a 2-layered drawing consists of placing nodes in the first node set V on a straight line L_1 and placing nodes in the second node set W on a parallel line L_2. The one-sided crossing minimization problem asks to find an ordering of nodes in V to be placed on L_1 so that the number of arc crossings is minimized. In this paper, we a 1.4664-approximation algorithm for this problem. This improves the previously best bound 3 due to P. Eades and N. C. Wormald [Edge crossing in drawing bipartite graphs, Algorithmica 11 (1994), 379-403].

11. P. Eades, Q. Feng, X. Lin, H. Nagamochi:
"Straight-Line Drawing Algorithms for Hierarchical Graphs and Clustered Graphs",

Algorithmica, （掲載予定）.

概要: Hierarchical graphs and clustered graphs are useful nonclassical graph models for structured relational information. Hierarchical graphs are graphs with layering structures; clustered graphs are graphs with recursive clustering structures. Both have applications in CASE tools, software visualization, and VLSI design. Drawing algorithms for hierarchical graphs have been well investigated. However, the problem of straight-line representation has not been solved completely. In this paper, we answer the question: does every planar hierarchical graph admit a planar straight-line hierarchical drawing? We present an algorithm that constructs such drawings in linear time. Also, we answer a basic question for clustered graphs, that is, does every planar clustered graph admit a planar straight-line drawing with clusters drawn as convex polygons? We provide a method for such drawings based on our algorithm for hierarchical graphs.

12. T. Ishii, H. Nagamochi, T. Ibaraki:
"Augmenting a $(k-1)$-Vertex-Connected Multigraph to an ℓ-Edge-Connected and k-Vertex-Connected Multigraph", Algorithmica, （掲載予定）.

概要: For two integers $k, \ell > 0$ and an undirected multigraph $G = (V, E)$, we consider the problem of augmenting G by the smallest number of new edges to obtain an ℓ-edge-connected and k-vertex-connected multigraph. In this paper, we show that a $(k-1)$-vertex-connected multigraph G can be made ℓ-edge-connected and k-vertex-connected by adding at most $\max\{\ell+1, 2k-4\}$ surplus edges over the optimum in $O(\min\{k, \sqrt{n}\}kn^3 + n^4)$ time, where $n = |V|$.

13. Y. Karuno, H. Nagamochi:
"Scheduling Vehicles on Trees", Pacific Journal of Optimization, （掲載予定）.

概要: The vehicle scheduling problem consists of a set of n jobs which are located at different vertices in a given graph. Each job is characterized by a release time, a handling time and a due date (or a deadline). There are m $(1 \leq m \leq n)$ identical vehicles on the graph to process the jobs. The problem asks to find a routing schedule of the m vehicles that minimizes a given objective function. Graphs are restricted to paths or trees in some applications, and thus the problem on these graphs has been studied extensively. In this paper, we give a brief review of approximation algorithms to the problem on paths or trees obtained by the previous work. As a closely related topic, we also discuss the subtree cover problem where a given edge-weighted tree with n weighted vertices is partitioned into a number of subtrees so as to minimize a given objective. In this paper, we propose an $O(n^3 \log n)$ time 3-approximation algorithm to the problem of minimizing the number of subtrees, where the weight of each subtree must not exceed a specified capacity.

14. H. Nagamochi:
"A $\frac{4}{3}$-Approximation for the Minimum 2-Local-Vertex-Connectivity Augmentation in a Connected Graph", J. Algorithms, （掲載予定）.

概要: Given a simple connected graph $G = (V, E)$ and a set R of pairs of vertices, we consider the problem of augmenting G by a smallest set F of new edges such that the resulting graph $G + F$ remains simple and has at least two internally disjoint paths between u and v for each pair $(u, v) \in R$. The problem is known to be NP-hard, and a 3/2-approximation algorithm has been obtained so far. In this paper, we introduce new stronger lower bounds on the optimal value, and propose an $O(|E|+|R|)$ time 4/3-approximation algorithm to the problem.

15. H. Nagamochi:
"Approximating the Minmax Rooted-Subtree Cover Problem", IEICE Transactions, (掲載予定).
概要: Let $G = (V, E)$ be a connected graph such that each edge $e \in E$ and each vertex $v \in V$ are weighted by nonnegative reals $w(e)$ and $h(v)$, respectively. Let r be a vertex designated as a root, and p be a positive integer. The minmax rooted-subtree cover problem (MRSC) asks to find a partition $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ of V and a set of p subtrees $T_1, T_2, \ldots, T_p$ such that each T_i contains $X_i \cup \{r\}$ so as to minimize the maximum cost of the subtrees, where the cost of T_i is defined to be the sum of the weights of edges in T_i and the weights of vertices in X_i. Similarly, the minmax rooted-cycle cover problem (MRCC) asks to find a partition $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ of V and a set of p cycles $C_1, C_2, \ldots, C_p$ such that C_i contains $X_i \cup \{r\}$ so as to minimize the maximum cost of the cycles, where the cost of C_i is defined analogously with the MRSC. In this paper, we first propose a $(3 - 2/(p+1))$-approximation algorithm to the MRSC with a general graph G, and we then give a $(6 - 4/(p+1))$-approximation algorithm to the MRCC with a metric (G, w).

16. 石井 利昌, 永持 仁, 高橋 健吾, 西垣 豊, 武田 真人:
"タンク繰りにおける経路探索法", システム制御情報学会誌, (掲載予定).
概要: 石油化学事業において, 石油化学プラントを効率的に運用するための生産計画の最適化が要求されている. 生産計画の最適化を考慮する際, プラントへ原料をいかに効率よく供給するかは, 重要な課題の一つである. 通常, 購入された原料は, まず, 港から一時的に複数の貯蔵用タンクに受け入れられ, その後生産計画に従って, プラントへ供給される. この際, 配管網上で, 港-タンク間, タンク-タンク間, またはタンク-プラント間において, 互いに途中の配管を共有しない 2 本以上の経路を見つけることが求められる. 本研究では, この配管網上での経路探索問題に対し, 配管網をグラフに置き換えることで, グラフ理論を用いた解法を提案する. 我々の解法では, 効率的に問題を解くために, 要求されうる全ての経路をあらかじめ木状のデータ構造に蓄える. 提案アルゴリズムの有効性については, 昭和電工 (株) における事例を基に, 計算機実験により検証する.

研究会等

1. H. Nagamochi and T. Kawada:
"Approximating the minmax subtree cover problem in a cactus", The 15th Annual International Symposium on Algorithms and Computation (ISAAC2004), Lecture Notes in Computer Science, 3341, 705-716, December 2004.
概要: Let $G = (V, E)$ be a connected graph such that edges and vertices are weighted by nonnegative reals. Let p be a positive integer. The minmax subtree cover problem (MSC) asks to find a partition $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ of V and a set of p subtrees $T_1, T_2, \ldots, T_p$, each T_i containing X_i so as to minimize the maximum cost of the subtrees, where the cost of T_i is defined to be the sum of the weights of edges in T_i and the weights of vertices in X_i. In this paper, we propose an $O(p^2 n)$ time $(4 - 4/(p+1))$-approximation algorithm for the MSC when G is a cactus. This is the first constant factor approximation algorithm for the MSC.

2. T. Ishii, H. Fujita, H. Nagamochi:
"Minimum cost source location problem with local 3-vertex-connectivity requirements", Computing: The Australasian Theory Symposium (CATS) Australasian Computer Science Week, 97-105, 30 January - 3 February, 2005.
概要: Let $G = (V, E)$ be a simple undirected graph with a set V of vertices and a

set E of edges. Each vertex $v \in V$ has a demand $d(v) \in Z_+$ and a cost $c(v) \in R_+$, where Z_+ and R_+ denote the set of nonnegative integers and the set of nonnegative reals, respectively. The source location problem with vertex-connectivity requirements in a given graph G asks to find a set S of vertices minimizing $\sum_{v \in S} c(v)$ such that there are at least $d(v)$ pairwise vertex-disjoint paths from S to v for each vertex $v \in V - S$. It is known that if there exists a vertex $v \in V$ with $d(v) \geq 4$, then the problem is NP-hard even in the case where every vertex has a uniform cost. In this paper, we show that the problem can be solved in $O(|V|^4(\log |V|)^2)$ time if $d(v) \leq 3$ holds for each vertex $v \in V$.

C07: Web コンテンツ活用に関連した離散最適化問題の研究

増山 繁 † 中山 慎一 ‡ 本間 宏利 § 相田 慎 †

† 豊橋技術科学大学知識情報工学系
〒 441-8580 豊橋市天伯町雲雀ヶ丘 1-1
{masuyama,aida}@tutkie.tut.ac.jp

‡ 徳島大学総合科学部
〒 770-8502 徳島市南常三島町 1-1
shin@ias.tokushima-u.ac.jp

§ 釧路工業高等専門学校 情報工学科
〒 084-0916 釧路市大楽毛西 2 丁目 32-1
honma@info.kushiro-ct.ac.jp

1 はじめに

本グループでは、Web 上に存在する膨大な量の情報を活用するための技術的問題を離散最適化問題として定式化し、それに対し、実用的観点からみて有効かつ適切なアルゴリズムを開発することを目的とする。特に、以下の 2 つの項目に重点をおいて研究を実施している。

1. 要約、検索などの、 Web コンテンツを知的活動において活用するのを支援するための基本技術の確立

2. Web コンテンツ配信方法を求める問題のグラフ理論的定式化とその解法

1 の細目は以下の通りである。

1.1. ユーザの個別の情報要求に適合した要約手法、及び、分類手法とそのアルゴリズムの開発

1.2. Web データから人間が気づかない未知の知識を発見、獲得する手法の開発

2 の細目は以下の通りである。

2.1. コンテンツ配信問題に対する計算量の解明と効果的解法の提案

2.2. コンテンツ配信の基盤となる、ネットワーク信頼性等、高度情報通信網に関連した諸問題の定式化とそのアルゴリズム

平成１６年度に得られた主な成果は以下のとおりである。

1. 要約、検索などの、Web コンテンツを知的活動において活用するのを支援するための基本技術の確立について

1.1. 自動要約の重要な要素技術である文圧縮において、エントロピー等を用いて、名詞の修飾の必要性を推定することで、削除可能な動詞連体修飾節の認定を行なう手法を考案した。

1.2. 複数文書要約において、要約対象となる文書集合からキーワードを抽出して、それをユーザに提示し、選択させるなどのインターラクションを導入してユーザの個別の情報要求に適合させる要約手法について研究した。

1.3. 可読性の向上を目的とした片仮名表記外来語の換言知識獲得について成果を得た。

2. Web コンテンツ配信方法を求める問題のグラフ理論的定式化とその解法、及び、その基盤となる高度情報通信網に関連した問題に関して

2.1. コンテンツ配信におけるサーバ配置やセンサネットワークにおけるデータ収集・処理用プロセッサの配置に関連した、最小節点ランキング全域木問題の計算量を解明し、更に置換グラフについて効率の良いアルゴリズムを得た。

2.2 コンテンツ配信の基盤となる高度情報通信網上での負荷分散に関連した問題のグラフ理論による定式化を試みた。

2.3 コンテンツ配信の基盤となる高度情報通信網上での非同期分散分枝限定法を定義し、その正当性と有限時間停止性を証明した。また、それのもつ可能性を論じた。

2 Web コンテンツ活用に関連した問題

2.1 動詞連体修飾節の省略可能性に関するコーパスからの 知識獲得

テキスト自動要約における文内要約の一要素技術として、動詞連体修飾節の省略可能性に関する

知識をコーパスから獲得する手法を提案した。具体的には、動詞連体修飾節が修飾している名詞に対して、修飾されやすさ、修飾多様性をコーパスから調べ、修飾される頻度が低い、若しくは、修飾する動詞の種類が限定されている名詞に係る動詞連体修飾節を省略可能と認定する。同時に、重要な内容を持つ名詞に係り、かつ、重要な内容を持たない動詞連体修飾節を省略可能と認定する。なお、修飾多様性を計るのにエントロピーを用いた。本手法によって省略可能と認定された動詞連体修飾節を評価したところ、再現率 69.4%において, 精度 77.3%との結果を得た。

近年のコンピュータと情報通信技術の進歩により、多くの情報を得ることができるようになった。しかし、それは同時に情報の氾濫を招き、その結果、文書情報を要約するテキスト自動要約の必要性が高まってきている。要約とは、人間がテキスト内容の理解、取捨選択をより容易にできるようにするために、元のテキストを短く表し直したものをいう。これまでの研究で提案されてきた要約手法は、ある文書集合に対して重要な文を抽出し文書を再構成する重要文抽出型の要約や、一文毎に不要箇所を認定し、その不要箇所を省略することで要約を行なう文内要約などがある。しかし、どのような使用目的の要約でも作成できる万能な手法は存在しないため、要約の使用目的に応じた手法を選択し、時には、複数の手法を併用して要約を作成することが必要となる。基本的には、ある文書集合に対して重要文抽出を行ない、その文に対していくつかの文内要約の手法を適用することで、要約文書を作成する要約システムを構築する。例えば、国立情報学研究所主催の情報検索、質問応答、文書要約の評価のためのワークショップ、NTCIR2 における要約タスク TSC 1 で好成績を収めた我々のシステム YELLOW[4] もこのような構成をしている。

テキスト自動要約における文内要約の目的は、重要文抽出で抽出された文を更に短縮し、要約率を下げることである。重要文抽出のみのテキスト自動要約システムでは、長い文が頻出する文書を要約する場合において、低い要約率が達成できない、もしくは、低い要約率を達成するために抽出可能な文数が少なくなり、要約文書に入れることができる情報が減少する。テキスト自動要約において、文内の情報欠落の少ない部分を削除することで重要文を更に短くし、なるべく多くの情報を入れるために、長い文を短くする文内要約技術が必要である。

本研究では、文内要約の一要素技術として、不要箇所省略による要約を実現するための一手法である、文中の省略可能な動詞連体修飾節を認定するために必要な知識をコーパスから獲得する手法を提案した。省略可能と認定された動詞連体修飾節を文中から削除することで、重要文抽出された文を、更に短い文にすることができる。よって、本手法を重要文抽出型の要約システムに組み込むことで、要約率を更に下げることができる。本研究における目標は、省略可能な動詞連体修飾節をできるだけ多く、かつ、高い精度で認定することである。そして、本研究で提案する手法によって、この目標は概ね達成可能である。

本研究では、形態素情報などのタグが付与されていない一般のコーパスから不要箇所省略による要約において利用できる言語知識を自動的に獲得し、それを用いて要約を行なう一手法を提案した。ここで、不要箇所の単位として連体修飾節の動詞連体修飾節（以降、動詞連体とする）に着目する。動詞連体とは、名詞を修飾している連体修飾の中で、動詞を含み、かつ、その動詞が名詞を修飾している連体修飾節と定義する。例えば、「大舞台で演技するスター」の「大舞台で演技する」は、名詞「スター」を修飾している動詞連体である。本手法では、動詞連体が修飾している名詞に対して、修飾され易さ、修飾多様性をコーパスから調べる。そして、修飾される頻度が低い、もしくは、修飾する動詞の種類が限定されている名詞に係る動詞連体を省略可能と認定する。また、動詞連体の内容、および、前後の文脈を考慮して、以下のような工夫を行なっている。

(1) その動詞連体に含まれている情報が以前の文にも含まれている情報である場合には、省略可能と認定され易くする。

(2) 重要な情報が含まれている場合には、省略可能と認定されにくくする。

なお, 修飾多様性を計るのに, エントロピーを用いる。本手法によって省略可能と認定された動詞連体修飾節を評価したところ、再現率 69.4%において、精度 77.3%との結果を得た [5]。

2.2 ユーザとのインタラクションを導入した複数文書システム

近年のコンピュータと情報通信技術の進歩により、多くの情報を得ることができるようになった。しかし、それは情報の氾濫を招き、そのことにより、文書情報を要約するテキスト自動要約の必要性が高まってきている。その中でも、複数の文書を自動要約する研究は、検索結果等の大規模な文書集合を大幅に縮めてひとつの文書として提供することにより迅速な理解を可能にする。そのため、その技術の確立が強く望まれており、近年、盛んに研究されている。複数文書要約とは、検索質問に適合する文書集合から指定された長さの要約を生成するタスクと定義される。ところが、検索質問に適合する複数の文書を要約するとはいえ、文書集合中や文書中の話題は一様ではない。たとえば、ソニーの AIBO の発売に関するものや販売方法に関するものなど様々な話題が含まれている。要約された文書は、これらの話題をすべて盛り込んでいることが望ましいが、少ない文字数では、すべてに対応することは困難である。そこで、多様な要約要求に対応するために、ユーザとのインタラクションを導入した複数文書要約システムを開発する。まず、要約対象となる文書集合から検索質問と関連したキーワードを自動的に抽出し、ユーザに指示する。次に、ユーザが情報要求に適したキーワードを選択、もしくは、適さないキーワードを削除し、選択したキーワードによって生成される要約文書を制御する。

本要約システムは、検索と要約の評価のためのワークショップ NTCIR4 における要約タスクに参加し、良好な評価結果を得た。但し、参加の際は、本システムで付されたスコアの上位から一定数キーワードを選択することで、インタラクションを導入せず自動要約システムとして参加し、評価を受けた [6]。

2.3 可読性の向上を目的とした片仮名表記外来語の換言知識獲得

本研究では、外来語である片仮名語、特に英語を語源とした片仮名語の和語または漢語への換言のための知識獲得に関する研究を行なった結果を報告した。近年、公的文書等における難解な片仮名語の乱用が問題視されている。片仮名語の大部分は英単語に基づく外来語であり、従来日本語で用いられてきた語彙に換言可能な場合も多い。換言とは、ある言語表現の意味内容を保持したまま別の表現へと言い替えることである。自然言語処理のための要素技術として今後ますます重要になると認識されている。換言するための知識は人手で作成することもできるが、実用的な質と量を満たすためには多大な労力を要する。そのため、換言知識は可能な限り自動的に獲得することが望ましい。以上より、本研究では、難解な片仮名語をより理解し易い語へと言い替えるための換言知識を自動的に獲得することを目的としている。手順としては、まず、片仮名語の元になった英単語を復元する。そして、得られた英単語の日本語訳を辞書によって獲得し、候補を絞り込む。実験の結果、英単語復元は再現率 82.2%、精度 81.1%を得、換言候補獲得については再現率 14.6%、精度 70.8%となった。

近年、日本語の公的文書において片仮名語が多用されるようになり、文書可読性の低下が問題となっている。国立国語研究所は、自治体の広報紙等で用いられることの多い難解な外来語である片仮名語に対して、より理解しやすい語への換言例を作成し、文書可読性の向上を推奨している。換言とは、ある言語表現の意味内容を保持したまま、別の表現へと言い替えることであり、その有用性が最近注目されている。同所は、今後も半年に５０語程度ずつ換言例を追加するとしている。このような手順をとっている理由としては、一度にすべての換言知識を整備することが困難であること、外来語である片仮名語には新語が多いため、ある時点で換言知識を十分に整備したとしても、次の年には知識の追加や更新が必要になること等があげられている。２００４年１２月現在で提案されている語は１４１語であり、日常的に用いられている片仮名語に比べると、はるかに少ない。より大量の換言知識を整備するために、全ての換言規則を人手で作成するのではなく、ある程度自動的に取得することが望ましい。

片仮名語からの換言知識の獲得を目的とした研究として、宮木らの名詞間類似度を用いた研究 [9] があげられる。名詞間類似度は、用いられる文脈

が似ている語は意味も似ているという仮定に基づき、共起する名詞を要素とするベクトル間の余弦によって定義される。

宮木らの研究では、名詞間類似度と換言可能性を同一のものとして扱っているが、実際には、異なっている場合も多い。例えば、「アップル」と「ぶどう」は、用いられる文脈が似ているため、名詞間類似度は高いが換言可能ではない。宮木らの手法では、上位概念語、関連語、反意語なども換言可能とみなされてしまう傾向にある。特に、宮木らは、上位概念語を換言可能であるとしているが、この判断は必ずしも適切ではないと考える。確かに、ある語からその上位概念語への換言を行なった場合、より広範な意味をもつ語になるため、間違った詳細情報が付加されることはない。しかし、換言処理の応用を考えると、一般には情報の変化だけではなく、情報の欠落も起こらないことが望ましい。上位概念語への換言は、原文の情報が抽象的になることで、詳細な情報の欠落が起こっていると考えられる。また、情報欠落の点を除いても、文脈によっては上位概念語に換言することが不適切な場合もあることから、上位概念語は必ずしも換言の正解例とすべきではないといえる。

以上を踏まえ、本研究では、片仮名語からの換言知識を自動獲得するための手法を考案した。その際に、片仮名語の性質に特化した手法を用いることで性能の向上を試みた。

換言知識の自動獲得の研究としては、他にも、パラレルコーパスを用いたものがある。しかし、一般に大量のパラレルコーパスを利用することは困難であり、獲得された換言知識の量は少ない。特に、片仮名語に関しては、パラレルコーパス自体が入手困難であるため、本研究では考慮していない。また、久光らは、括弧表現を利用して換言事例を自動獲得している。この方法も、獲得される知識の量は多くないが、単一のコーパスから知識獲得が可能であることや、獲得された知識の正解率が高いこと等の利点もある。そのため、本研究では、この研究に基づく手法も併用している。

換言の必要がある片仮名語の大部分は、英語に基づく外来語である。つまり、その片仮名語が日本語の語彙中では新語・未知語だったとしても、元となった英単語は、英語の語彙中で既知の場合が多い。そのため、日英翻訳のための辞書を用いて、英単語から日本語訳を獲得することができる。そこで、片仮名語から元になった英単語を復元する。一般に、ひとつの英単語に相当する日本語訳は、数十語程度獲得されるので、その中から最もふさわしい一語に絞り込むために、統計的手法を併用する。英単語が復元できなかった場合の換言候補はコーパス中の全名詞とする。以上が、本手法の主要部分の概要である。また、難解な片仮名語は新聞記事中で補足説明されている場合がある。本手法では、これらの情報も利用し、換言知識獲得の手助けとした。

実験の結果、英単語復元は再現率 82.2%, 精度 81.1%を得、換言候補獲得については再現率 14.6%、精度 70.8%となった [10]。

3 Web コンテンツ配信と関連した問題、および、その基盤としての高度情報通信網に関連した問題

3.1 最小節点ランキング全域木問題の計算複雑度

グラフ G の節点ランキングとは、同じラベルをもつ任意の 2 節点を結ぶ路上に必ず両端の節点のラベルより大きなラベルをもつ節点が存在するように節点にラベルを振ることである。グラフ G の節点ランキングのうち、最大ラベルが最小となるものを最小節点ランキングという。与えられたグラフの全域木のうち、最小節点ランキングが最小となるものを求める問題を最小節点ランキング全域木問題 (MVRST: minimum vertex ranking spanning tree) という。この問題は、VLSI 設計、データ配信におけるサーバの配置問題、センサネットワークにおけるデータ処理プロセッサの配置等への応用が考えられる。

まず、3 次元マッチング問題が決定問題版の MVRST へ多項式時間帰着可能であることを示すことにより、MVRST が NP 困難であることを示した。また、グラフ G の、直径が最小となる全域木を求めるというアイデアに基づいた近似率 $\frac{\lfloor \frac{1}{2}(\ell+3) \rfloor}{\lceil \log_2(\ell+2) \rceil}$ の近似アルゴリズムを提案した [2]。

一方、置換グラフに対し、長さ 4 以上の単純閉路を含まないなどの性質を用いることで、動的計

画法に基づく $O(n^3)$ 時間のアルゴリズムを開発した [3]。

3.2 モバイルエージェント実行計画問題について

モバイルエージェント実行計画問題を定式化し、各エージェントの通信するエージェント数を２に制限した場合ですら強 NP 完全であることを証明した。また、NP 完全である範囲や、近似アルゴリズムについての検討を行なった。

マルチエージェントシステムは、特に人工知能の分野で精力的に研究されてきた。エージェントとはプロセスなどのような動作主体 (computational entity) のことである。モバイルエージェントとは、任意のホストに移動可能なエージェントのことで、分散環境におけるプロセスマイグレーションの概念とほぼ同じである。マルチエージェントシステムにおけるモバイルエージェントの移動性に関する研究は、通信コストの削減を目的としている。しかし、あるホストに膨大な数のエージェントが集中すればそのホストは過負荷となることより、CPU コストと通信コストの両方のバランスをとるようにホストにエージェントを配置することによって、効率的な実行を目指すことが必要になる。通常、CPU コストの最大値を最小にするように設計されたこの種の配置最適化は、マルチプロセッサ上でのタスクスケジューリングの形式で表される。よって、よって、モバイルエージェントタスクに対応させ、ホストをプロセッサに対応されることにより、モバイルエージェントの負荷分散を達成することを、マルチプロセッサにおけるタスクスケジューリングの拡張とみなすことができる。しかし、従来のタスクスケジューリング問題では、モバイルエージェントの相互通信と移動について考慮することはできない。そこで、新たにこのような問題をモバイルエージェント実行計画問題として定義して、その計算複雑度を解析する。

マルチプロセッサ上のタスクスケジューリングは３０年以上の間研究されている。従来の研究では、CPU コストのバランスをとることや、タスク間の関係（半順序関係など）が着目されてきた。また、従来の研究により、タスクが preemptive でなければ問題はマルチプロセッサスケジューリングとなり、強 NP 完全となることが知られている。なお、タスクが preemptive の場合は、多項式時間で最適なスケジュールを得ることができる。

その一方で、モバイルエージェントシステム上でのシステム全体の観点からの負荷分散の研究は全くされてこなかった。この理由はエージェントが自律的存在であるためだと推察される。エージェントの移動の最適化に関して従来からいくつかの研究がなされているが、それらはすべて個々のエージェント移動に焦点を当てて研究したもので、システム全体の性能に関する研究ではない。例えば、データのリモートアクセス、メッセージ交換、プロセスマイグレーションの性能比較、一連のタスクのためのエージェント移動スケジュールタスクとエージェントの旅程 (itinerary) を考慮したモバイルエージェントの選択などである。これらは、モバイルエージェントの相互通信を考えずに、エージェントとホストとの相互通信のみを考え、エージェントの移動スケジュールのみを最適化しようとしたものである。システム管理エージェントに関しては、そのような定式化は適切であり有用であるが、実際の多くのエージェントシステム（たとえば、情報交換や契約など）では、エージェントの相互通信を必要とする。もちろん、エージェント間での通信に関する研究（たとえば、契約ネットなど）は多く行なわれているが、これらの研究は負荷分散に焦点を合せていない。

システム全体の性能向上を目指すのは、個々のエージェント利益を平均的に良く保つと予想できることより妥当である。そこで、システム全体の仕事の完了時間を最小にすることを目的とする、モバイルエージェントの相互通信に関する要素を定式化に取り込む。

モバイルエージェントは preemptive タスクとみなすことができる。よって、エージェント間に通信が全くないなら、多項式時間で最適な配置を得ることができる。しかし、エージェントが互いに通信するとき、これを得ることができるかどうかは分かっていない。本研究では、エージェントがお互いに通信する場合には、時間最適な配置を求めることは強 NP 完全であることを証明した。具体的には、CPU コストと実行途中のエージェントの移動の考慮を不要にし、さらに、各エージェントの通信相手が丁度二つのエージェントになる

ように制限した問題が強 NP 完全であることを証明した。通常、エージェントは限られた数 ($O(1)$) のエージェントとのみ通信するため、この制限は現実のモバイルエージェントシステムの環境を反映している。この成果は、エージェントがお互いに通信する必要があるほぼすべての実際の状況に対し、最適なエージェントの配置を与えるどのような効率的なアルゴリズムもないであろうということを示したことになる [7]。

3.3 非同期分散分枝限定法の提案

分散システムにおいて、各変数がタスクに対応し、その値がそのタスクの割り当て先ホストを示すような負荷分散問題を解くための新しい非同期分散分枝限定法を提案する。これは、NP 困難な離散最適化問題に対して非同期完全分散システムで近似解でない厳密な最適解を求める最初の最適化分散アルゴリズムである。これは従来の分散最適化アルゴリズムに比べて高い柔軟性と頑健性をもつ。そのアイデアには、分枝限定法、分割統治法、および、局所探索法における λ-Opt 近傍の考え方を複合させている。本手法は、今後の拡張により、大規模動的分散システムにおいて有用になり得る。

負荷分散、資源配分、施設配置などは分散システムを頑健、柔軟、かつ、効率良く運用するための基本的な問題である。これらの問題に対して従来から逐次、分散の双方において数多くの研究が行なわれている。これらの問題の多くは NP 困難であるが、最適化という観点からは、逐次環境では数多くの研究が存在するのに対し、分散環境では最適解を求める研究は非常に少なく、ほとんどがアドホックな近似解法の研究である。これは、大規模分散システムにおいて、これらの問題の最適解を求めることが逐次の場合よりも更に困難であることに起因していると推測される。具体的には、分散システムでは大域的な情報の扱いやシステム全体の合意形成が困難であったり非常に手間がかかったりするためである。そのため、従来提案されているほとんどすべての分散環境下での手法は、局所的な情報のみを用いる局所探索法の一種である。従って、ある時点で局所最適解に到達してしまうと、処理する時間的余裕があるにもかかわらず、それ以上の改善が期待できない。そのため、実行途中で近似解が求まり、かつ、最終的には大域的な最適解が求まる手法は有用と考えられる。更に、地理的分散システムにおいては、耐故障性、動的な変化（タスクの動的な到着等）への対応、大規模システムへの対応なども必要である。柔軟性や頑健性の観点からはこれらの性質の方が手法の時間・通信複雑度や得られる解の精度よりも重要な場合もある。本稿では、上記の性質をすべて満たす可能性を秘めている非同期分散分枝限定法を提案し、その可能性を探る。今回は、最も基本的な枠組の提案に留まるが、今後の継続的な研究により、より有用性の高い手法へと発展することが期待される。

今回提案する非同期分散分枝限定法は、従来の逐次環境での分枝限定法（例えば、[Ibaraki 87][1] 参照）に基づいている。しかし、それだけでなく、他の手法の考え方も取り入れている。まず、ホスト間で協調して分枝操作を行なうために分割統治法における統合の考え方を利用している。また、局所的な状態から順に解が検討されていくため、局所探索法の λ-Opt 近傍の振舞に似た動作をする。その結果、非同期分散分枝限定法の動作は、逐次環境の分枝限定法と比較して大きく異なっているようにみえる。最も大きな違いは、逐次の分枝限定法の動作は唯一の分枝木に基づいてアルゴリズムの実行が進むが、今回提案した非同期分散分枝限定法では各ホストがひとつずつ独立した分枝木をもち、それらが非同期に協調してアルゴリズムの実行が進むことである。この違いが、単純に逐次の分枝限定法を分散化しただけの手法にはない有用な性質を与えている [8]。

参考文献

[1] Toshihide Ibaraki, Enumerative Approaches to Combinatorial Optimization, Part I, II, J. C. Baltzer AG, 1987.

[2] 宮田敬三, 増山繁, 中山慎一, “最小節点ランキング全域木問題の計算複雑度”, 第 17 回 回路とシステム軽井沢ワークショップ論文集, pp.645-650, 2004.

[3] Shin-ichi Nakayama, Shigeru Masuyama, “An $O(n^3)$ Time Algorithm for Obtaining the Minimum Vertex Ranking Spanning Tree on Permutation Graphs”, Proc. of the 4th Japanese-Hungarian Symposium on Discrete Mathematics and its Applications, 掲載予定.

[4] 大竹清敬, 岡本大吾, 児玉充, 増山繁, “重要文抽出, 自由作成要約に対応した新聞記事要約システム YELLOW”, 情報処理学会論文誌「データベース」, Vol.43, No.SIG 2(TOD 13), pp.37-47, 2002.

[5] 酒井 浩之, 増山 繁, “動詞連体修飾節の省略可能性に関するコーパスからの 知識獲得”, 電子情報通信学会論文誌 D-II, Vol.J87-D-II, No.8, pp.1641-1652, 2004 年 8 月.

[6] Hiroyuki Sakai, Shigeru Masuyama, “‘A Multiple-Document Summarization System with User Interaction”, Proceedings of Coling2004, Vol.II, pp.1001-1007, August, 2004.

[7] Atsushi Sasaki, Tadashi Araragi, Shigeru Masuyama, Keizo Miyata, “Formulation of Mobile Agents Allocation and its Strong NP-Completeness”, IEICE Trans. Fundamentals, 掲載予定.

[8] 佐々木淳, 櫟粛之, 増山繁, “An Asynchronous Distributed Branch and Bound for Load Balancing(負荷分散のための非同期分散分枝限定法)”, 電子情報通信学会技術研究報告 COMP2004-63, pp.23-32, 2005.

[9] 宮木衛, 酒井 浩之, 吉田辰巳, 増山 繁, “片仮名語からの換言候補の自動獲得”, 情報アクセスのためのテキスト処理シンポジウム発表論文集 (電子情報通信学会「言語理解とコミュニケーション」研究会主催), pp.96-103, 2003.

[10] 吉田辰巳, 遠間　雄二, 増山 繁, 酒井 浩之, “可読性の向上を目的とした片仮名表記外来語の換言知識獲得”, 電子情報通信学会論文誌 D-II, 掲載予定.

研究業績一覧

学術論文

1. 酒井 浩之, 増山 繁:
“動詞連体修飾節の省略可能性に関するコーパスからの 知識獲得”, 電子情報通信学会論文誌 D-II, Vol.J87-D-II, No.8, pp.1641-1652, 2004 年 8 月.
概要: テキスト自動要約における文内要約の一要素技術として, 動詞連体修飾節の省略可能性に関する知識をコーパスから獲得する手法を提案した. 具体的には, 動詞連体修飾節が修飾している名詞に対して, 修飾されやすさ, 修飾多様性をコーパスから調べ, 修飾される頻度が低い, 若しくは, 修飾する動詞の種類が限定されている名詞に係る動詞連体修飾節を省略可能と認定する. 同時に, 重要な内容を持つ名詞に係り, かつ, 重要な内容を持たない動詞連体修飾節を省略可能と認定する. なお, 修飾多様性を計るのに, エントロピーを用いる. 本手法によって省略可能と認定された動詞連体修飾節を評価したところ, 再現率 69.4%において, 精度 77.3%との結果を得た.

2. Hiroyuki Sakai, Shigeru Masuyama:
“A Multiple-Document Summarization System with User Interaction”, Proceedings of Coling2004, Vol.II, pp.1001-1007, August, 2004.
概要: We propose a multiple-document summarization system with user interaction. Our system extracts keywords from sets of documents to be summarized and shows the keywords to a user on the screen. Among them, the user selects some keywords reflecting his/her needs. Our system controls the produced summary by using these selected keywords. For evaluartion of our method, we participated in TSC3 of NTCIR4 workshop by letting our system select 12 best keywords as scored by our system. Our entered system attained the best performance in content evaluation among

systems not using sets of questions. Moreover, evaluation of user interaction shoed that the interaction is effective.

3. Atsushi Sasaki, Tadashi Araragi, Shigeru Masuyama, Keizo Miyata:
"Formulation of Mobile Agents Allocation and its Strong NP-Completeness", IEICE Trans. Fundamentals, (掲載予定).
概要: We formally define the mobile agent allocation problems from a system-wide viewpoint and then prove that it is strongly NP-complete even if each agent communicates only with two agents. This is the first formal definition for acheduling mobile agents from the viewpoint of load balancing, which enables us to discuss its properties on a rigorous basis. The problem is recognized as preemptive scheduling with independent tasks that require mutual communication. The result implies that almost all subproblems of mobile agent allocation, which require mutual communication agents, are strongly NP-complete.

4. 吉田辰巳, 遠間　雄二, 増山 繁, 酒井 浩之:
" 可読性の向上を目的とした片仮名表記外来語の換言知識獲得", 電子情報通信学会論文誌 D-II, (掲載予定).
概要: 本論文では, 外来語である片仮名語, 特に英語を語源とした片仮名語の和語または漢語への換言のための知識獲得に関する研究を行なった結果を報告した. 近年, 公的文書等における難解な片仮名語の乱用が問題視されている. 片仮名語の大部分は英単語に基づく外来語であり, 従来日本語で用いられてきた語彙に換言可能な場合も多い. 換言とは, ある言語表現の意味内容を保持したまま, 別の表現へと言い替えることである. 自然言語処理のための要素技術として, 今後ますます重要になると認識されている. 換言するための知識は人手で作成することもできるが, 実用的な質と量を満たすためには多大な労力を要する. そのため, 換言知識は可能な限り自動的に獲得することが望ましい. 以上より, 本研究では, 難解な片仮名語をより理解し易い語へと言い替えるための換言知識を自動的に獲得することを目的としている. 手順としては, まず, 片仮名語の元になった英単語を復元する. そして, 得られた英単語の日本語訳を辞書によって獲得し, 候補を絞り込む. 実験の結果, 英単語復元は再現率 82.2%, 精度 81.1%を得, 換言候補獲得については再現率 14.6%, 精度 70.8%となった.

5. Shin-ichi Nakayama, Shigeru Masuyama:
"n $O(n^3)$ Time Algorithm for Obtaining the Minimum Vertex Ranking Spanning Tree on Permutation Graphs", Proc. of the 4th Japanese-Hungarian Symposium on Discrete Mathematics and its Applications, (掲載予定).
概要: The minimum vertex ranking spanning tree problem is to find a spanning tree of G whose vertex ranking is minimum. This paper proposes an $O(n^3)$ time algorithm for solving the minimum vertex ranking spanning tree problem on a permutation graph.

研究会等

1. 宮田敬三, 増山繁, 中山慎一:
"最小節点ランキング全域木問題の計算複雑度", 第 17 回 回路とシステム軽井沢ワークショップ論文集, 2004 年 4 月, pp.645-650.
概要: グラフ G の節点ランキングとは, 同じラベルをもつ任意の 2 節点を結ぶ路上に必ず両端の節点のラベルより大きなラベルをもつ節点が存在するように節点にラベルを振ることである. グラフ G の節点ランキングのうち, 最大ラベルが最小となるものを最小節点ランキングという. 与えられたグラフの全域木のうち, 最小節点ランキングが最小となるものを求める問題を最小節点ランキング問題（MVRST と略称する）という. 本稿では MVRST の NP 困難性を証明した。更に、近似率 $\frac{\lfloor \frac{1}{2}(\ell+3) \rfloor}{\lceil \log_2(\ell+2) \rceil}$ の近似アルゴリズムを提案した.

2. Yasuo Nii, Keizo Kawata, Tatsumi Yoshida, Hiroyuki Sakai, Shigeru Masuyama:
"Question Answering System QUARK", Working Notes of NTCIR Workshop 4 Meeting, pp.367-372, 2004年6月.
概要: Recently, we can acquire immence amount of information thanks to the spread of a computer and internet. Therefore, technology for finding the information that a user desires becomes more and more important. A question answering (QA) system answers a question written by natural language in contrast to conventional information retrieval systems where a user expresses his information need by keywords. Therefore, a QA system can provide more user-friendly information access environment to a user. We developed a QA system QUARK(QUestion AnsweRing system using a large corpus as a Knowledger source) that finds answer words from large newspaper article corpora and was evaluated by participating in NTCIR4 QAC2, an evaluation workshop of Japanese QA sytems.

3. Hiroyuki Sakai, Shigeru Masuyama:
"A Multiple-Document Summarization System introducing User Interface for reflecting User's Summarization Need", Working Notes of NTCIR Workshop 4 Meeting, pp.444-451, 2004年6月.
概要: We propose a multiple-document summarization system with user interaction. Our system extracts keywords from sets of documents to be summarized and shows the keywords to a user on the screen. Among them, the user selects some keywords reflecting his/her needs. Our system controls the produced summary by using these selected keywords. For evaluartion of our method, we participated in TSC3 of NTCIR4 workshop by letting our system select 12 best keywords as scored by our system. Our entered system attained the best performance in content evaluation among systems not using sets of questions. Moreover, evaluation of user interaction shoed that the interaction is effective.

4. Masanobu Tsuruta, Yoshiyuki Umemura, Hiroyuki Sakai, Shigeru Masuyama:
"A Web Search Result Classification System based on the Degree of Suitability for Specialists ", Working Notes of NTCIR Workshop 4 Meeting (Supplement), Vol.1, pp.45-50, 2004年6月.
概要: We propose a search result classification system based on the degree of suitability for specialists. Our system classifies documents based on whether a document is "for specialists" or "not for specialists", respectively. This classification is done by ranking each document using the density of keywords and by a threshold. For evaluation od our system, we participated in NTCIR4 WEB Topical Classification Task. Only a part of "evaluation based on distribution of relevant documents" has executed on this occasion. As a result, our system exhibits good performance for some data set. We also independently conducted experiments for evaluation based on classification errors. Experimental results show that the precision of classification of our system attains value close to that of average by human evaluators'.

5. 佐々木淳, 櫟粛之, 増山繁:
" An Asynchronous Distributed Branch and Bound for Load Balancing(負荷分散のための非同期分散分枝限定法)", 電子情報通信学会技術研究報告, COMP2004-63, pp.23-32, 2005年1月.
概要: We propose a new asynchronous distributed branch and bound algorithm for a load balancing problem in which each variable corresponds to each task and indicates a host,where the corresponding task is assigned, in a geographically distributed system. This is the first algorithm to pro-

vide the exact optimum solution, not an approximation, for NP-hard discrete optimization problems in a distributed context without any centralized control. Moreover, this algorithm has more flexibility and greater robustness than the conventional distributed algorithms. The idea behind the algorithm is a complex consisting of branch and bound, divide and conquer, and λ-Opt neighborhood in local search. This algorithm has a possibility to be useful in an actual huge dynamic distributed system.

6. 佐々木淳，宮田敬三，櫟粛之，増山繁:
“ モバイルエージェント実行計画問題について”，京都大学数理解析研究所 数理科学講究録 (2004 年度冬の LA シンポジウム), 2005 年 2 月発表, 講究録掲載予定.
概要: モバイルエージェント実行計画問題を定義し, 各エージェントの通信するエージェント数を 2 に制限した場合ですら強 NP 完全であることを証明した．また, NP 完全である範囲や, 近似アルゴリズムについての検討を行なった.

7. 佐々木淳，櫟粛之，増山繁:
“ 非同期分散分枝限定法の基本構造と可能性”, 第 18 回 回路とシステム軽井沢ワークショップ, （発表予定）.
概要: 分散システムにおいて, 各変数がタスクに対応し, その値がそのタスクの割り当て先ホストを示すような負荷分散問題を解くための新しい非同期分散分子限定方を提案する. これは, NP 困難な離散最適化問題に対して非同期完全分散システムで近似解でない厳密な最適解を求める最初の最適化分散アルゴリズムである．これは従来の分散最適化アルゴリズムに比べて高い柔軟性と頑健性をもつ. そのアイデアには, 分枝限定法, 分割統治法, および, 局所探索法における λ-Opt 近傍の考え方を複合させている．本手法は, 今後の拡張により, 大規模動的分散システムにおいて有用になり得る.

学会大会等

1. Atsushi Sasaki, Tadashi Araragi, Shigeru Masuyama:
“Proposal of Asynchronous Distributed Branch and Bound”, Workshop on New Horizons in Computing, 2005 年 3 月.

2. 梅村祥之, 辻貞治, 増山繁:
“文書読解時視点移動パターンからの興味に関する感性情報の抽出の試み”, 言語処理学会第 11 回年次大会発表論文集, pp.141-144, 2005 年 3 月.

3. 太田貴久, 増山繁:
“模倣レポート判定支援システムの開発”, 言語処理学会第 11 回年次大会発表論文集, pp.141-144, 2005 年 3 月.

4. 鶴田雅信, 梅村祥之, 酒井浩之, 増山繁:
“Web 検索結果の専門家に対する適合度によるランキング手法について”, 言語処理学会第 11 回年次大会発表論文集, pp.1018-1021, 2005 年 3 月.

C08: 高性能近似アルゴリズムの設計法に関する研究

平田　富夫 †　藤戸　敏弘 ‡　小野　孝男 †

† 名古屋大学 大学院 情報科学研究科
〒 464-8603 名古屋市千種区不老町
{hirata,ono}@is.nagoya-u.ac.jp

‡ 豊橋技術科学大学 情報工学系
〒 441-8580　豊橋市天伯町雲雀ヶ丘 1-1
fujito@ics.tut.ac.jp

1　はじめに

グラフ問題や組合せ問題のような離散構造をもつ問題のほとんどは NP 完全（最適化問題の場合は NP 困難）であり, 現在の計算機では計算時間が膨大になり手に負えない問題である．しかし, たとえ NP 困難であっても, 計算機を用いてなんとか解かなければならない離散最適化問題が情報処理の現場ではますます増えている．たとえば, OR の分野では, より大規模なネットワーク上での資源割当て問題やスケジューリング問題を解かなければならない．また, 人工知能の分野では推論処理のような高度な計算を要求する問題がつぎつぎと発生している．このような現実を踏まえ, たとえ求まる解が最適ではなくとも, それに十分近いことを保証できる近似アルゴリズムの設計論が今日の重要な研究テーマとなっている．本研究の目的は, グラフの彩色問題と集合被覆問題を中心とした代表的離散最適化問題に対する高性能近似アルゴリズムを開発するとともに, これまでに提案されている近似アルゴリズムを設計手法の立場から調査・分類し一般的設計法を構築することである．

本年度の研究成果は以下のようである．

グラフ問題に関しては次のような成果をあげた。均等辺彩色問題の高性能アルゴリズムを開発した。重み付き独立集合問題に対する近似アルゴリズムを開発した。ネットワーク設計問題に対する組合せ的近似アルゴリズムを開発した。頂点被覆問題と木状被覆問題に対する並列アルゴリズムを開発した。木状被覆を求めるための主双対法を提案した。さらに、被覆容量／要求量付き部分頂点被覆問題の 2 倍近似解法を与えた。

集合問題に関しては次のような成果をあげた。被覆型 0-1 整数計画問題と部分集合被覆問題に対し、組合せ的近似アルゴリズムの提案と解析を行った。集合多重被覆問題および集合充填問題の高性能近似アルゴリズムを開発した．

この他, 公開鍵暗号系において重要な演算であるスカラー倍計算の効率的なアルゴリズムを与えた．また, 3 次元離散ボロノイ図を効率よく求めるアルゴリズムとそのハードウェアアルゴリズムを提案した．以下にその詳細を述べる．

2　グラフ問題

各種のグラフ・ネットワーク問題に対して以下のようなアルゴリズムを設計し解析した．

均等辺彩色問題の高性能アルゴリズム

この問題は, グラフの各頂点においてそこに接続する辺の色が各色ほぼ同じ数になるように色を塗る問題である．1982 年にオイラー閉路を用いた $O(kn^2)$ 時間のアルゴリズムが提案され, その後, $O(n^2/k + n|V|)$ に改善された．ここで, n は頂点数, k は使用する色数である．本研究では $O(n^2/k)$ 時間のアルゴリズムを与えた．このアルゴリズムのアイデアは, 彩色の途中で使用する色数を各色とも常にほぼ同数にするという平衡条件 (balanced condition) にある [8].

重み付き独立集合問題に対する近似アルゴリズム

グラフの独立集合とは頂点の部分集合でどの 2 点も辺で結ばれていないものをいう．独立集合問題では与えられたグラフ中の最大サイズの独立集合を見つける．この問題は NP 困難なため近似アルゴリズムの研究がなされており, 頂点数のほかに最大次数や平均次数を用いて近似率が解析されてきた．しかし, 重み付きの問題では平均次数をパラメータとした近似率の解析はなされていなかっ

た. 重み付きの場合, 入力のグラフに対し重みの小さい頂点を多数加えて, 最適解を変えずに平均次数を任意に小さくすることができてしまうためである. これを回避するために, 本論文では, 平均次数を拡張した重み付き平均次数を提案し, それを用いて近似率を解析した.　さらに, 重み付き inductiveness というパラメータを定義し, それを用いた解析も行った [11].

{2,3}-EC-SNDP に対する近似アルゴリズム

ネットワーク設計問題のひとつに Survival Network Design Problem(SNDP) がある. {2,3}-EC-SNDP は, グラフと, その各頂点対に対し 2 または 3 の確保すべき枝連結度が与えられたとき, その要求を満たすような最小の部分グラフを得る問題である. この問題に対しては線形計画法を繰り返し用いた 2 近似アルゴリズムが知られているが, その時間計算量は多項式時間とはいえ実用的なものではない. 本研究では深さ優先探索と極大全域森を組み合わせたグラフ論的手法によるアルゴリズムを提案した. その近似比率が $\frac{7}{3}$ となることを示し, さらに, このアルゴリズムを改良し近似比率が 2 となることを示した [12].

頂点被覆問題と木状被覆問題に対する NC アルゴリズム

グラフの頂点被覆問題はよく知られた NP-困難な組合せ最適化問題である. ここでは, 無向グラフが与えられたとき, 全ての辺について少なくともどちらか一方の端点を含むような頂点部分集合のうち, 含まれる頂点の重みの合計が最小であるものが求められる. これまで同問題には, 各頂点が被覆できる辺数に制限を加えたり, ある決められた割合いの辺数だけ被覆することを要求するなどの一般化が個々に考えられてきた. 本研究では, 辺や頂点に関するこれらの被覆条件を併せもつ一般化問題を新たに導入し, 劣モジュラ集合被覆アルゴリズムを拡張することで, この問題に対して多項式時間で近似度 2 が保証できることを示した [1].

グラフの木状被覆（あるいは連結辺支配集合）問題とは, 連結グラフが与えられたとき, 連結な辺部分集合で, その外部にあるどの辺にも接続しているものの中から, 最小なものを計算する問題である. これは, 通常の頂点被覆であることに加え, 連結部分グラフを誘導するような頂点集合を計算する問題としてとらえることもできる. 同問題は NP 困難で, 頂点被覆問題と同等以上に近似計算が困難である. 頂点被覆には, いくつかの 2 倍近似 NC アルゴリズムが知られているのに対し, 連結頂点被覆には, 近似保証のある並列アルゴリズムが存在しない. しかも, 既存の 2 倍近似逐次アルゴリズムを並列化しても, 高計算量の RNC アルゴリズムにしかならない. 本研究では, 連結頂点被覆ならびに木状被覆に対し, 2 倍近似 NC ならびに RNC アルゴリズムを開発した. 入力グラフの頂点数 n, 辺数 m, 最大次数 Δ とすると, この NC アルゴリズムは EREW-PRAM 上で $O(\Delta^2(m+n)/\log n)$ 個のプロセッサを用いて $O(\log^2 n)$ 時間で並列実行でき, RNC アルゴリズムは, CRCW-PRAM 上で $O(m+n)$ 個のプロセッサを用いて期待値 $O(\log n)$ の時間で並列実行できる.

木状被覆を求めるための主双対法

重みつき木状被覆（あるいは連結辺支配集合）問題では, 辺コストをもつ連結グラフが与えられ, 最小コストの連結辺支配集合を計算することが求められる. 関連問題である頂点被覆や辺支配集合が, 一般コストを許しても 2 倍近似可能であるのに対し, 木状被覆は一様コストの場合にのみ 2 倍近似アルゴリズムが知られていた. 一般コストの木状被覆に対する最良近似保証は $3+\epsilon$ であり, しかも楕円体アルゴリズムを必要とする. 本研究では, 2 倍以上の開きがある 2 種類のコストのみが許された木状被覆に対し, 主双対法に基づく 2 倍近似アルゴリズムを開発した [4].

被覆容量／要求量付き部分頂点被覆問題の 2 倍近似解法

本研究では, 生産計画問題のひとつとして, 容量つき需要-供給問題（CSD）を新たに導入し, その問題構造を解析するため, 従来の劣モジュラ集合被覆問題（SSC）の部分集合に関する制約を整数ベクトルに関するものに拡張した, 劣モジュラ整数被覆問題（SIC）の検討を提案した. 主双対法に基づく SSC に対する近似アルゴリズムを SIC に対するものに発展させ, その性能解析を CSD に適用することで, CSD のネットワーク構造のみに依存し, 数値データに依存しない近似保証が得られることを示した [5].

3　集合問題

集合被覆問題および集合充填問題の高性能アルゴリズムを開発した.

被覆型 0-1 整数計画問題と部分集合被覆問題

被覆型 0-1 整数計画問題と部分集合被覆問題, およびそれらの特別な場合に対し, 線形計画丸め法や半正定値計画丸め法といった, 高計算量を要する手法を用いた近似アルゴリズムが近年数多く開発されている. 本研究では, より高効率で純粋に組合せ的なアルゴリズムについて, その近似性能を検証した. 丸め法を用いて得られた最良結果と比較すると, その性能はいくつかの特別な場合で劣るものの, 一般には同等以上の性能を有し, 重み付き多重被覆, 部分集合被覆, および更なる一般化問題では, その性能が優っていることを示した [2].

集合多重被覆問題に対する貪欲法の改良

集合多重被覆問題とは, 台集合 U とその部分集合の族が与えられたとき, U の各要素 u を含む部分集合が, 予め決められた数 r_u 以上に属している族のうち, 最小なものを計算する問題で, 通常の集合被覆問題（$r \equiv 1$ に相当）を一般化するため NP 困難である. 与えられた部分集合の最大サイズを k とするとき, この問題は貪欲法により $H_k = \sum_{i=1}^{k}(1/i)$ 倍以内で近似されることが知られていたが, より良い近似保証は存在しなかった. 本研究では, 貪欲法を改良して近似度 $H_k - 1/6$ が保証できることを示した [6].

重みつき集合充填問題に対する局所改善法

互いに素な部分集合からなる集合族をパッキングというが, 重みつき集合パッキング問題とは, 重みつき部分集合の族が与えられたとき, それに含まれる部分集合の重み和を最大化するパッキングを計算するという, よく知られた NP 困難な最適化問題である. 特に与えられた部分集合の最大サイズが k であるとき, k 集合パッキング（k-SP）という. 本研究では, 部分集合の重みが 1 と w に制限された k-SP（但し, $w \geq 2.5$）に対し, 局所探索法の一種であり, 重みなし集合パッキング問題に対し有効であることが知られている t-local search アルゴリズムを拡張して適用し, 近似度 $\frac{k(k-1)^s-2}{2(k-1)^s-2}$（但し, $t = 2s$）が保証できることを示した [7].

4　その他

この他, 公開鍵暗号系において重要な演算であるスカラー倍計算の効率的なアルゴリズムを与えた. また, 3 次元離散ボロノイ図を効率よく求めるアルゴリズムとそのハードウェアアルゴリズムを提案した.

スカラー倍計算の効率的なアルゴリズム楕円曲線上のスカラー倍計算の基本演算は加算 $P+Q$ と 2 倍算 $2P$ である. ここで, P, Q は楕円曲線上の点である. スカラー倍計算の基本的な計算法として Window 法があり, その中では 2^kP+Q という形の計算が反復される. 本研究では, この 2^kP+Q を効率良く計算する方法 (直接計算) を提案し, これを Window 法に適用することで, 従来よりも計算時間を削減した [9]. さらに, 直接計算に座標の切り替えというアイデアを適用して計算時間の改良をおこなった [13]. また, モンゴメリのトリックを用いて計算時間を改善した [15, 16].

3 次元離散ボロノイ図を求めるアルゴリズム

3 次元離散ボロノイ図とは 3 次元 2 値画像のボロノイテセレーションのことである. つまり, 3 次元空間内に何個かの生成点が与えられたとき, 各画素についてそこからもっとも近い生成点を見つける問題である. 本研究ではこれに対し $O(N^3)$ 時間の最適アルゴリズムをあたえた. ただし, 画像サイズは $N \times N \times N$ である. さらに, これをハードウェアアルゴリズムとして実現した. これは $O(N^3)$ 個のセルアレーを用い $O(N^2)$ 時間で 3 次元離散ボロノイ図を求める [10].

参考文献

[1] Fujito, T., Doi, T., “A 2-Approximation NC Algorithm for Connected Vertex Cover and Tree Cover,” *Information Processing Letters*, Vol. 90, No. 2, pp. 59–63, 2004.

[2] 藪田隆俊, 藤戸敏弘, “被覆容量／要求量付き部分頂点被覆問題の 2 倍近似解法”, 電子情報通信学会論文誌 D-I, Vol. J87-D-I, No. 11, pp. 1–8, 2004.

[3] Fujito, T., “On Combinatorial Approximation of Covering 0-1 Integer Program and

Partial Set Cover", *J. Combinatorial Optimization*, Vol. 8, No. 4, pp. 439–452, 2004.

[4] Doi, T., Fujito, T., "A Primal-Dual Method for Approximating Tree Cover with Two Weights," *Proc. 3rd CTW Workshop on Graphs and Combinatorial Optimization*, pp. 119–123, 2004.

[5] Fujito, T., Yabuta, T., "Submodular Integer Cover and its Application to Production Planning," *Lecture Notes in Computer Science*, Vol. 3351, pp. 154–166, 2005.

[6] 倉橋秀和, 藤戸敏弘, "集合多重被覆問題に対する貪欲法の改良", 電子情報通信学会 コンピュテーション研究会技術研究報告 COMP2004-61, pp. 9–16, 2005.

[7] 大竹将知, 藤戸敏弘, "重みつき集合充填問題に対する局所改善法について", 電子情報通信学会 コンピュテーション研究会技術研究報告 COMP2004-62, pp. 17–22, 2005.

[8] Xie, X., Ono, T., Hirata, T, "An improved algorithm for the nearly equitable edge-coloring proble" *Trans. of IEICE on Fundamentals*, Vol. E87-A, No. 5, pp. 1029–1033, 2004.

[9] 安達大亮, 蒲生真之, 平田富夫, "直接計算による楕円曲線上のスカラー倍計算の効率化", 電子情報通信学会論文誌, Vol. J88-A, No. 1, pp. 54–61, 2005.

[10] Hirata, T., "3-D Voronoi tessellation algorithms" *Japan Journal of Indusatrial and Applied Mathematics*, Vol. 22, No. 2, 2005.
A preliminary version has appeared in *Proc. of International Symposium on Voronoi Diagrams in Science and Engineering*, Tokyo, pp. 173–178, 2004.

[11] 加古明久, 小野孝男, 平田富夫, Halldorsson, M., "重み付き独立集合問題に対する近似アルゴリズム", 情報処理学会アルゴリズム研究会研究報告, AL99, pp. 55–62, 2005.

[12] 勝谷裕樹, 小野孝男, 平田富夫, "グラフ論的手法を用いた {2,3}-EC-SNDP に対する近似アルゴリズムの研究", 電子情報通信学会コンピュテーション研究会技術研究報告, comp2004-60, pp. 1–8, 2005.

[13] 安達大亮, 平田富夫, "座標系の切替えと直接計算によるスカラー倍計算の効率化", 電子情報通信学会暗号と情報セキュリティシンポジウム (SCIS2004), pp. 1013-1018, 2004.

[14] 安達大亮, 平田富夫, "楕円曲線上のスカラー倍計算の効率化", 京都大学数理解析研究所講究録 1375, pp. 195-200, 2004.

[15] 安達大亮, 平田富夫, "モンゴメリのトリックを用いた 2^kP 倍点の改良計算法", 情報処理学会アルゴリズム研究会, AL98, pp. 33-40, 2004.

[16] 安達大亮, 平田富夫, "Refined Computations for Points of the form 2^kP Based on Montgomery Trick", 電子情報通信学会暗号と情報セキュリティシンポジウム (SCIS2005), pp. 1117-11122, 2005.

研究業績一覧

学術論文

1. X. Xie, T. Ono, T. Hirata:
"An improved algorithm for the nearly equitable edge-coloring problem", Trans. of IEICE on Fundamentals, Vol. E87-A, No. 5, pp. 1029–1033, 2004, 5.
概要: A nearly equitable edge-coloring of a multigraph is a coloring such that edges incident to each vertex are colored equitably in number. this problem is solved in $O(kn^2)$ time, where n and k are the numbers of the edges and the colors, respectively. The running time was improved to be $O(n^2/k + n|V|)$ later. We present a more efficient algorithm for this problem that runs in $O(n^2/k)$ time.

2. 安達大亮, 蒲生真之, 平田富夫:
“直接計算による楕円曲線上のスカラー倍計算の効率化”, 電子情報通信学会論文誌, Vol. J88-A, No. 1, pp. 54–61, 2005, 1.
概要: 楕円曲線上のスカラー倍計算の基本演算は加算 $P+Q$ と 2 倍算 $2P$ である. ここで, P, Q は楕円曲線上の点である. スカラー倍計算の基本的な計算法として Window 法があり, その中では 2^kP+Q という形の計算が反復される. 本論文では, この 2^kP+Q を効率良く計算する方法を提案し, これを Window 法に適用することで, 従来よりも計算時間を削減する.

3. T. Hirata:
“3-D Voronoi tessellation algorithms”, Japan Journal of Indusatrial and Applied Mathematics, Vol. 22, No. 2, 2005.
概要: We consider the discrete Voronoi diagram in the three-dimensional space, that is, the Voronoi tessellation of a 3-D binary image. The input to the tessellation algorithm is a 3-D image containing a set of pixels of value 0 (generators). The goal is to classify the rest of the pixels to the nearest generator. This paper gives a simple algorithm for computing the Voronoi tessellation map of a 3-D binary image. It runs in $O(N^3)$ time for an $N \times N \times N$ input image. A hardware algorithm is also presented, which computes the 3-D Voronoi tessellation map in $O(N^2)$ time on an $O(N^3)$-cell array.

4. T. Fujito, T. Doi:
“A 2-Approximation NC Algorithm for Connected Vertex Cover and Tree Cover”, Information Processing Letters, Vol. 90, No. 2, pp. 59–63, 2004.
概要: The connected vertex cover problem is a variant of the vertex cover problem, in which a vertex cover is additional required to induce a connected subgraph in a given connected graph. The problem is known to be NP-hard and to be at least as hard to approximate as the vertex cover problem is. While several 2-approximation NC algorithms are known for vertex cover, whether unweighted or weighted, no parallel algorithm with guaranteed approximation is known for connected vertex cover. Moreover, converting the existing sequential 2-approximation algorithms for connected vertex cover to parallel ones results in RNC algorithms of rather high complexity at best. In this paper we present a 2-approximation NC (and RNC) algorithm for connected vertex cover (and tree cover). The NC algorithm runs in $\mathrm{O}(\log^2 n)$ time using $\mathrm{O}(\Delta^2(m+n)/\log n)$ processors on an EREW-PRAM, while the RNC algorithm runs in $\mathrm{O}(\log n)$ expected time using $\mathrm{O}(m+n)$ processors on a CRCW-PRAM, when a given graph has n vertices and m edges with maximum vertex degree of Δ.

5. 藪田隆俊, 藤戸敏弘:
“被覆容量／要求量付き部分頂点被覆問題の 2 倍近似解法”, 電子情報通信学会論文誌, Vol. J87-D-I, No. 11, pp. 1–8, 2004, 11.
概要: グラフの頂点被覆問題はよく知られた NP-困難な組合せ最適化問題である. ここでは, 無向グラフが与えられたとき, 全ての辺について少なくともどちらか一方の端点を含むような頂点部分集合のうち, 含まれる頂点の重みの合計が最小であるものが求められる. これまで同問題には, 各頂点が被覆できる辺数に制限を加えたり, ある決められた割合の辺数だけ被覆することを要求するなどの一般化が個々に考えられてきた. 本稿では辺や頂点に関するこれらの被覆条件を併せもつ一般化問題を新たに導入し, 劣モジュラ被覆アルゴリズムを拡張することで, この問題に対して近似率 2 が多項式時間で保証できることを示す.

6. T. Fujito:
“On Combinatorial Approximation of Covering 0-1 Integer Program and Partial Set Cover”, J. Combinatorial Optimization,

Vol. 8, No. 4, pp. 439–452, 2004.
概要: The problems dealt with in this paper are generalizations of the set cover problem, $\min\{cx \mid Ax \geq b, x \in \{0,1\}^n\}$, where $c \in Q_+^n, A \in \{0,1\}^{m \times n}, b \in \vec{1}$. The covering 0-1 integer program is the one, in this formulation, with arbitrary nonnegative entries of A and b, while the partial set cover problem requires only $m-K$ constrains (or more) in $Ax \geq b$ to be satisfied when integer K is additionally specified. While many approximation algorithms have been recently developed for these problems and their special cases, using computationally rather expensive (albeit polynomial) LP-rounding (or SDP-rounding), we present a more efficient purely combinatorial algorithm and investigate its approximation capability for them. It will be shown that, when compared with the best performance known today and obtained by rounding methods, although its performance comes short in some special cases, it is at least equally good in general, extends for partial vertex cover, and improves for weighted multicover, partial set cover, and further generalizations.

7. T. Doi, T. Fujito:
"A Primal-Dual Method for Approximating Tree Cover with Two Weights", Proc. 3rd CTW Workshop on Graphs and Combinatorial Optimization, pp. 119–123, 2004.
概要: The *tree cover (TC)* problem is to compute a minimum weight edge set, given a connected and edge-weighted graph G, s.t. its vertex set forms a vertex cover for G. Unlike related problems of vertex cover or edge dominating set, weighted TC is not yet known to be approximable in polynomial time as good as the unweighted version is. Moreover, the best approximation algorithm known so far for weighted TC is far from practical in its efficiency. In this paper we consider a restricted version of weighted TC, as a first step towards better approximation of general TC, where only two edge weights differing by at least a factor of 2 are available. It will be shown that a factor 2 approximation can be attained efficiently (in the complexity of max flow) in this case by a primal-dual method. Even under the limited weights as such, the primal-dual arguments used will be seen quite involved, having a nontrivial style of dual assignments as an essential part in it, unlike the case of uniform weights.

8. T. Fujito, T. Yabuta:
"Submodular Integer Cover and its Application to Production Planning", Lecture Notes in Computer Science, Vol. 3351, pp. 154–166, pp. 154–166, 2005.
概要: Suppose there are a set of suppliers i and a set of consumers j with demands b_j, and the amount of products that can be shipped from i to j is at most c_{ij}. The amount of products that a supplier i can produce is an integer multiple of its capacity κ_i, and every production of κ_i products incurs the cost of w_i. The *capacitated supply-demand (CSD)* problem is to minimize the production cost of $\sum_i w_i x_i$ such that all the demands (or the total demand requirement specified separately) at consumers are satisfied by shipping products from the suppliers to them. To capture the core structural properties of CSD in a general framework, we introduce the *submodular integer cover (SIC)* problem, which extends the *submodular set cover (SSC)* problem by generalizing submodular constraints on subsets to those on integer vectors. Whereas it can be shown that CSD is approximable within a factor of $O(\log(\max_i \kappa_i))$ by extending the greedy approach for SSC to CSD, we first generalize the primal-dual approach for SSC to SIC and evaluate its performance. One of the approximation ratios obtained for CSD from such an approach is the maximum number of suppliers that can ship to

a single consumer; therefore, the approximability of CSD can be ensured to depend only on the network (incidence) structure and not on any numerical values of input capacities κ_i, b_j, c_{ij}. The CSD problem also serves as a unifying framework for various types of covering problems, and any approximation bound for CSD holds for set cover generalized *simultaneously* into various directions. It will be seen, nevertheless, that our bound matches (or nearly matches) the best result for each generalization *individually*. Meanwhile, this bound being nearly tight for standard set cover, any further improvement, even if possible, is doomed to be a marginal one.

研究会等

1. 加古明久, 小野孝男, 平田富夫, M. Halldorsson:
“重み付き独立集合問題に対する近似アルゴリズム”, 情報処理学会アルゴリズム研究会研究報告, AL99, 55–62, 2005, 1.
概要: 重みなし最大独立集合問題の近似アルゴリズムの近似率は, 頂点数, 最大次数, 平均次数などをパラメータとして解析されている. しかし, 重み付きの問題では平均次数をパラメータとした近似率の解析はなされていない. 本論文では, 平均次数を拡張した重み付き平均次数と重み付き inductiveness というパラメータを導入し, それを用いて近似率を解析する.

2. 勝谷裕樹, 小野孝男, 平田富夫:
“グラフ論的手法を用いた {2,3}-EC-SNDP に対する近似アルゴリズムの研究”, 電子情報通信学会コンピュテーション研究会技術研究報告, comp2004-60, 1–8, 2005, 1.
概要: ネットワーク設計問題のひとつに Survival Network Design Problem(SNDP) と呼ばれる問題がある. 本研究では, {2,3}-EC-SNDP に対し, 深さ優先探索と極大全域森を組み合わせたアルゴリズムを提案し, その近似比率が $\frac{7}{3}$ となることを示す. また, このアルゴリズムを改良し近似比率が 2 となることを示す.

3. 倉橋秀和, 藤戸敏弘:
“集合多重被覆問題に対する貪欲法の改良”, 電子情報通信学会コンピュテーション研究会技術研究報告, COMP2004-61, pp. 9–16, 2005, 1.
概要: 集合多重被覆問題は組合せ最適化問題の一種であり, NP 困難な問題として知られている. この問題は台集合 U の部分集合の族 $\mathcal{S}$ が与えられたとき, すべての要素について前もって与えられた要求カバー数 r_u 以上を含むような部分族 C でサイズが最小のものを求める問題である. 部分集合の最大サイズを k とすると, この問題は貪欲法によって $H_k = \sum_{i=1}^{k}(1/i)$ 倍以内で近似できることが知られている. 本稿では貪欲法の改良を提案し, 近似率 $H_k - 1/6$ が保証できることを示す.

4. 大竹将知, 藤戸敏弘:
“重みつき集合充填問題に対する局所改善法について”, 電子情報通信学会コンピュテーション研究会技術研究報告, COMP2004-62, pp. 17–22, 2005, 1.
概要: 重みつき集合充填問題とは, 重みのついた部分集合の族が与えられたとき, 互いに素な部分集合からなる族のうち重み最大のものを見つける問題である. 特に部分集合の最大サイズが k である問題を k-set packing problem（k-SP）という. 本稿では, 局所探索法の一種である t-local search アルゴリズムを利用し, 部分集合の重みが 1 と w に制限された k-SP（但し, $w \geq 5/2$）に対し, 近似比率が $\frac{k(k-1)^s-2}{2(k-1)^s-2}$（但し, $t = 2s$）の近似アルゴリズムを提案する.

5. 安達 大亮、平田 富夫:
“モンゴメリのトリックを用いた 2^kP 倍点の改良計算法”, 情報処理学会アルゴリズム研究会研究報告, AL98, pp. 33–40, 2004, 11.
概要: この論文では素体上で定義された楕円曲線に注目する。我々は、アフィン座標系において、楕円曲線上の点 P からその 2^k 倍の点 2^kP を求めるアルゴリズムを 2 つ提案

する。1つは $k = 2$ の場合に有効であり、もう1つは任意の自然数 k に対して有効である。これらのアルゴリズムは、素体上の逆元計算1回を素体上の乗算数回と置き換えることに基礎を置いている。我々は、逆元計算の置き換えにモンゴメリのトリックと呼ばれる技法を用いた。妥当な仮定の下で、我々のアルゴリズムは既存のアルゴリズムよりも効率良く動作する。

6. 安達 大亮、平田 富夫:
"Refined Computations for Points of the form $2^k P$ Based on Montgomery Trick", 暗号と情報セキュリティシンポジウム（SCIS2005）, pp. 1117–1122, 2005, 1.
概要: This paper focuses on algorithms for an efficient scalar multiplication. We propose two algorithms for computing points of the form $2^k P$ in affine coordinates. One works for $k = 2$, and the other works for arbitrary natural number k. The efficiency of these algorithms is based on a trade-off between a field inversion and several field multiplications. We apply Montgomery trick to implement this trade-off. Since a field inversion is usually more expensive than 10 field multiplications, our algorithms are efficient in comparison with existing ones.

C09: ネットワーク問題のモデル化とアルゴリズムの研究

伊藤 大雄 † 岩間 一雄 † 増澤 利光 ‡ 宮崎 修一 § 堀山 貴史 †

† 京都大学 大学院 情報学研究科
〒 606-8501 京都市左京区吉田本町
{itohiro,iwama,horiyama}@kuis.kyoto-u.ac.jp

‡ 大阪大学 大学院 情報科学研究科
〒 560-8531 豊中市待兼山町 1-3
masuzawa@ist.osaka-u.ac.jp

§ 京都大学 学術情報メディアセンター
〒 606-8501 京都市左京区吉田本町
shuichi@media.kyoto-u.ac.jp

1 はじめに

グラフは接続関係を表現する抽象モデルとして有用であり、古くから盛んに研究されている数学的対象である。特に近年は、計算機やインターネットの急速な発展に伴い、これらを対象としたグラフ問題に対するアルゴリズム研究が盛んになってきている。例えば、ネットワークの信頼性やルーティングの効率化、論理回路の最小化や基盤への埋め込みと言った問題はその典型例である。

本研究の目的は、ネットワークや計算機上での問題をグラフ問題としてモデル化し、そのアルゴリズム開発の研究を行うことである。ただし、本研究では、例えばルーティング問題を取り扱う場合にはルータの構造を特徴付けるグラフのみを考えるなど、入力を現実的なものに絞ることにより、アルゴリズムの効率化を目指している。以下、各節で、平成 16 年度の結果を述べる。

2 平坦なネットワークに対するルーティングアルゴリズム

本研究では、コンパクトルーティング問題と最大伸張度削減問題の二つを扱った。前者は一般的なルーティングに対して条件を緩和する事でコストを改善するアルゴリズムを構築する問題であるのに対して、後者は枝追加により効率的な全域木を構築する問題である。

コンパクトルーティングとは、基本的なネットワークルーティング問題のひとつであり、必ずしも最短経路でルーティングしない事によって必要とするテーブルサイズを削減する手法である。迂回経路とその最短経路の比を伸張係数と呼ぶが、近年、簡単かつ現実的なネットワークモデル下で伸張係数 3 かつテーブルサイズ $O(n^{2/3}\log^{4/3} n)$ を実現するコンパクトルーティングアルゴリズムが Cowen によって提案され、後に $O(\sqrt{n\log n})$ に改善された。この伸張係数 3 は一般的な場合の下限に一致する。しかし、平均的なネットワークが持っているような性質を考慮に入れると状況が変わって来る。我々はそのような性質を表すものとして平坦性と言う概念を導入し、与えられたネットワークが擬似平坦であるならば、伸張係数を大幅に改善でき伸張係数 $s < 3$ かつテーブルサイズ $O(\sqrt{n\log n})$ のアルゴリズムが存在する事を示した。

二つ目の最大伸張度削減問題はグラフの全域木を対象としている。全域木の計算は非常に一般的な問題でありネットワークルーティングに加えて様々な応用が存在するが、一般のグラフでは全域木が元のグラフの性質をほとんど表せないような都合の悪いグラフが考えられる。この近似度を最大伸張度として表現し、我々はグラフに新たに枝を追加した場合にどれだけ最大伸張度を削減できるかについて考察した。本研究では、(i) リンググラフに対して k 本枝追加で最適な最大伸張度削減アルゴリズム、(ii) 格子グラフに対して格子構造を保ったまま、最大伸張度を削減できるほぼ最適なアルゴリズム、(iii) 一般のグラフに対してグラフの最大伸張度 s の全域木が与えられていても、1 本枝追加で最大伸張度を 1 でも削減可能かどうかの判定が NP 困難である事、またその近似

度について、(iv) 一方で比較的多くの枝を追加した場合、最大伸張度を少なくとも 1 つ削減できるような多項式時間アルゴリズムが存在する事を示した。

3 孤立したクリーク発見問題

Web から情報を得る手法には、Yahoo! や Google のようにテキストに基づく検索手法と、HITS や PageRank などのようにリンクの構造に基づく手法がある。リンク構造に基づく検索手法は、あるページ u から v へのリンクがあるならば u の作者にとって v の内容が有用であろうという予想に基づいている。このようなリンク構造に基づいた情報検索手法としてグループ内で密にリンクされている Web ページのグループを見つけるというものがある。

この問題のアイデアは、そのような Web ページ群は互いに類似した内容を扱うページ群なのではないかというものである。リンク構造に基づく手法は、Web ページを頂点、Web リンクを枝に対応させた Web グラフと呼ばれるグラフを用いて議論されるが、密にリンクされている Web ページ群の Web グラフ上での例としてクリーク（完全部分グラフ）が挙げられる。しかしクリークを求める問題（最大のものを求める、極大のものを列挙する）のほとんどは難しく、良い近似方法も知られていない。

本研究では「孤立した」クリークを定義し、その発見問題を議論する。部分グラフが「孤立している」とは、内部で密にリンクされているだけでなく、その部分グラフと外部とのリンクが少ないことをいう。例えばサイズ k のクリークは、外部への枝が $k-1$ 本以下であるとき孤立しているという。また、c を定数とすると、外部への枝が $ck-1$ 本以下であるようなクリークを c-孤立クリークという。本研究では、このような孤立条件により多くの問題が簡単になり、孤立したクリークを列挙する問題を多項式時間で解くことができることを示した。また、孤立したクリークよりやや密度の低い擬クリークについても、平均次数が $k-\log k$ 以上でかつ最小次数が $\frac{k}{\log k}$ 以上である擬クリークを多項式時間で列挙できることを示した。

さらに、孤立したクリークを列挙するアルゴリズムを実装し、サイト間グラフと呼ばれる実際の Web から得られたグラフを用いて実験を行った。サイト間グラフとは、サイトを頂点、サイト間のリンクを枝に対応させたグラフである。これによりサイト内リンクを無視でき、Web のより巨視的な部分構造を調べることができる。我々はこのサイト間グラフから 6,974 個の孤立したクリークを発見し、類似した内容を扱うページ群であることを確認した。

4 最大被覆供給点配置問題に対する近似アルゴリズム

k を正整数とする。グラフにおいて供給点と呼ばれる節点の集合を定めたときに、$k-1$ 本の辺を任意にグラフから除去しても供給点集合と節点 v との間にパスが必ず確保されるとき、供給点は節点 v をカバーすると呼ぶ。この概念はネットワークの耐故障性を計る尺度として重要であり、この尺度を用いた問題として供給点配置問題が知られている。供給点配置問題とは、与えられたグラフの全ての節点をカバーするような最小要素の供給点配置を決定する問題であり、耐故障性に優れたネットワークを実現する上で重要な問題である。

本研究では、この問題と深い関係を持つ最大被覆供給点配置問題という問題を提案した。この問題は、与えられたグラフに対し、限られた数の供給点を配置して最大数の節点をカバーする問題である。本問題は、配置可能なサーバ数に制限がある場合での耐故障性に優れたネットワーク設計に重要となる。これら二つの問題は、集合被覆問題と最大被覆問題という二つの NP 困難問題と同様の関係を持っており、前者には供給点配置問題、後者には最大被覆供給点配置問題が対応する。なお、集合被覆問題と最大被覆問題では近似困難性が異なる。

供給点配置問題では多項式時間アルゴリズムが既に知られている。研究の目標は、最大被覆供給点配置問題に対する多項式時間アルゴリズムの発見、もしくは NP 困難性の証明である。本研究では、本問題にある制限を施すことで種々の多項式時間アルゴリズムを与えた。まず $k=2$ という制限の下で、連結グラフに対する多項式時間アルゴ

リズムを与えた。次に、非連結グラフに対する多項式時間アルゴリズムが連結グラフに対するものに還元できることを一般的に示し、その結果の一つとして、$k = 2$ の場合の非連結グラフに対する多項式時間アルゴリズムを得た。また、入力を木と高連結なグラフに制限した本問題に対しそれぞれ多項式時間アルゴリズムを与えた。

さらに本研究では、本問題を一般化した二つの問題が NP 完全であることを示した。一つは入力を有向グラフとした問題である。もう一つは、供給点の配置コストが各節点に与えられているとして、配置できる供給点を数ではなくコストによって制限した問題である。なお、これらと同様の一般化を供給点配置問題に施した場合においては多項式時間アルゴリズムの存在が示されている。

5 直径が制限された単位円グラフ上の様々な問題に対する多項式時間アルゴリズム

単位円グラフとは 2 次元平面上に配置された半径の等しい複数の円がグラフの頂点と一対一で対応し、2 つの円が交わる (あるいは接する) とき、またそのときに限りそれらの円と対応する 2 頂点が枝で連結されることによって得られるグラフである。グラフの直径とはそのグラフに含まれる頂点間の最大距離を指す。本研究ではグラフの直径が制限された単位円グラフにおける最小支配集合問題、最小連結支配集合問題、最大独立集合問題 (最小節点被覆問題)、孔発見問題、定数彩色問題に対する多項式時間アルゴリズムを与えた。

単位円グラフにおいてグラフの直径を制限することは単位円グラフを構築する領域のサイズを制限することを意味する。このような制限された領域は例えば災害などによって基地局が破壊されたような場で構築されるアドホックネットワークのモデルとして考えることができる。そのため本研究では円形の領域に配置された単位円集合をモデルとする単位円グラフについて議論したが、いずれの結果も一般的な領域に拡張するのは容易である。

また、このような直径への制限がグラフの入力パターン数をも制限してしまうことがないことも示した。つまり定数サイズの領域から得られる単位円グラフは直感的には座標が近い単位円に対応する頂点を一つの重みつき頂点として、有限個のグラフに置き換えることが出来そうであるが、それが不可能であることを証明した。

直径が制限された単位円グラフの頂点集合 V は、それぞれの頂点集合からなる誘導部分グラフが完全グラフとなるような、定数個 (例えば p 個とする) の部分集合へ分割することができる。そのため、最小支配集合、最小連結支配集合はそれぞれ $O(n^{p+1})$、$O(n^{2p-1})$ で発見できる。

最大独立集合問題に関しては単位円詰め込み問題と関係が深く、面積が a である円に重なりなく (円全体を領域の内部へ) 内包できる単位円の数は高々 $\frac{a}{2\pi}$ であることから、面積が a である領域から得られた任意の単位円グラフの最大独立集合は $O(n^{\frac{a}{2\pi}+1})$ で求めることができる。

孔 (弦のない閉路) 発見問題は、k が定数として与えられている場合には、サイズ k 以上の弦のない閉路をグラフが含むかどうかを判定する多項式時間アルゴリズムが知られている。しかし、k が問題の入力である場合、例えば最大孔発見問題などは NP 完全となる。単位円グラフにおける孔発見問題も一般には NP 完全であるが、グラフの直径を制限することによって多項式時間で解けるようになる。本研究では単位円グラフにおけるこの問題の NP 完全性の証明を与えた後、直径が制限された単位円グラフの場合に最大独立集合のサイズが弦のない閉路のサイズをおさえられることを利用し、$O(n^{\frac{a}{\pi}+0.376})$ で面積が a であるモデルから得られた任意の単位円グラフの孔を発見するアルゴリズムも与えた。

単位円グラフにおける彩色問題は、3-彩色の場合でも NP 完全となることが知られている。しかし、直径を制限した場合には領域の面積によって k-彩色可能な場合の頂点数が抑えられることから、領域の面積が定数でかつ k が定数として与えられている場合、定数時間での彩色が可能となる。また、領域の面積が $\log n$ で制限されている場合には、ある定数 k に対して多項式時間でグラフを k-彩色するアルゴリズムが存在することも同様に言える。しかし、直径が制限された単位円グラフの最小彩色数を求める多項式時間アルゴリズムはまだ知られていない。

6 H-彩色問題の計算複雑さの階層

H-彩色問題とは、色同士の彩色時の規則をグラフ H で表すことで従来の点彩色問題に自然な一般化を施した問題である。同問題はチャネルの割当て問題やスケジューリング問題、文法形式との関係など多方面で点彩色問題に比べより実用的な応用が可能であり、幅広い視点から積極的に研究がなされている。一般の H-彩色問題は特殊な場合を除き NP 困難であることが知られており、実用的な時間で厳密な解を得るアルゴリズムは存在しがたい。H-彩色問題に制限を与えた様々な問題についてもそれらの計算複雑さは明らかにされており、そのほとんどが NP 困難である。一方、平面グラフの H-彩色問題に関してはその計算複雑さは未解決である。

このような状況を踏まえ、本研究では平面グラフの H-彩色問題についての計算複雑さの解明に主眼を置き、任意の平面グラフが 4-彩色可能であるにも関わらず 3-彩色が NP 困難になるという、従来の点彩色問題における計算時間のギャップに着目し、その中間に相当する H-彩色問題の計算複雑さの解析を行った。Circulant graphs の部分クラスを用い、従来の n-彩色と $n+1$-彩色の間をより細かく分ける階層構造を示し、その階層構造について 2-彩色と 4-彩色の間にあたるいくつかの彩色問題の NP 困難性を証明した。特に 2-彩色に極めて近く、真に強力な彩色であるが、NP 困難である問題の存在を明らかにした。また、3- 彩色と 4-彩色の中間に位置する長さ 7 の閉路の補グラフによる平面彩色問題についてはその NP 困難性の証明とともに、3-彩色できないが長さ 7 の閉路の補グラフでは彩色できる平面グラフのクラスを定義し、そのクラスを長さ 7 の閉路の補グラフで彩色する線形時間アルゴリズムも与えた。

7 NP 完全問題に対する例題生成法

理論計算機科学の分野において、P=NP 問題は最も重要な未解決問題のひとつである。30 年にわたってこの困難な問題に対して、多方面から研究が行われている。NP 完全問題はその中でも中心的な位置を占めており、下限の研究、確率的手法、近似アルゴリズムなどの様々な成果が上げられている。ここでは、例題生成という観点からこの問題について研究した。

まず初めに、基本的な NP 完全問題のひとつである充足可能性問題について考察した。我々は、与えられた論理式 f に対して、充足可能性を保存しつつ解の密度を濃縮した論理式 g を生成することを目標とし、3-CNF 式の充足可能性判定アルゴリズムに基づき、解密度の濃縮アルゴリズムを 3 つ提示した。また、各アルゴリズムの濃縮度に関する議論を行った。評価手法として論理式の解の密度 d と比 $|g|/d$ を用い、充足可能性問題に対する良いアルゴリズムが必ずしも解の濃縮につながるとは限らないことを示した。

次に、グラフの彩色可能性問題について考察した。k-彩色不能なグラフをすべて網羅的に生成可能なグラフ算法として、Hajós calculus が知られている。任意の 3 彩色不能なグラフが多項式回の規則の適用で生成できるならば、NP = co-NP となる。しかし、現在のところ多項式回の規則の適用では生成できないようなグラフは知られていない。この問題に対するアプローチとして、我々は平面グラフ上の算法に着目し、$\mathcal{PHC}$ と $\mathcal{PHC}^*$ の 2 つを提示した。平面グラフ上の算法とは、生成するグラフの系列がすべて平面グラフであるものをいう。我々は、$\mathcal{PHC}$ と $\mathcal{PHC}^*$ が 3 彩色不可能な平面グラフを生成する健全かつ完全な系であることを証明し、それらがグラフを構成するのにかかるステップ数に関する評価を行った。また、$\mathcal{PHC}^*$ が $\mathcal{PHC}$ を多項式倍の規則の適用で模倣できることを示した。

8 最小頂点被覆問題に対する近似アルゴリズム

最小頂点被覆問題 (以下 VC) は古くから知られている NP 困難問題の中の一つである。この問題が $2-\epsilon$ 近似のアルゴリズムを持つか否かは極めて重要性の高い未解決問題であり、そのようなアルゴリズムは存在しないであろうと強く信じられている。我々は以下のように VC の入力に制限を加えた部分問題を考え、2 を大きく下回る近似度のアルゴリズムを与えることに成功した。

8.1 密なグラフ上の VC

MAX-SNP に含まれる多くの問題は入力を密なインスタンスに制限すると PTAS を持つことが知られているが、VC にはこれは当てはまらず、VC は密なグラフ上でも PTAS を持たない。しかしながら、密なグラフ上では 2 を大きく下回る近似度を与えることができる。我々は密なグラフ上の VC に対し、以下の様な確率的近似アルゴリズムを与えた。

(i) 我々のアルゴリズムは Karpinski と Zelikovsky による近似アルゴリズムを改良し、$2/(1+\Delta/d)$ の近似度を与えた。ここで δ はグラフの最大次数、d は平均次数を表す。

(ii) Karpinski らのアルゴリズムは d が $O(n)$ のときのみ動作するが、我々のアルゴリズムは $O(n \log\log n/\log n)$ の場合にも同様の近似度を与えることができる。

(iii) 我々の結果は以下の意味で最適である：もしより良い結果が存在するならば、一般の場合に $2-\epsilon$ の近似度が得られる。

8.2 完全マッチングを持つグラフ上の VC

マッチングと頂点被覆の間には強い関連があることが古くから知られている。Chen と Kanj は完全マッチングを持つグラフ上での VC(以下 VC-PM) を考え、(i) $1.069+0.069d$ (d は入力グラフの平均次数) の近似アルゴリズム、(ii) VC-PM は一般の VC と同程度に近似困難であること、を示した。我々は Chen らのアルゴリズムを改良し、近似度が $2-6.74/(d+6.28)$ のアルゴリズムを与えることに成功した。このアルゴリズムはより広い範囲の d で 2 を下回る近似度を与えることができている。

9 安定結婚問題に対する近似アルゴリズム

安定結婚問題とは、Gale と Shapley によって提唱されたマッチング問題である。この問題では、N 要素同士の 2 つの集合 (例えば、男性と女性) と、各個人の異性に対する希望リストが与えられる。男性 m が女性 w_2 よりも w_1 の方を好む時、$w_1 \succ_m w_2$ と表記する。また、マッチング M に対して男性 m とマッチしている相手の女性を $M(m)$ と表記する。ここで、あるマッチング M において、$w \neq M(m)$ であり、$w \succ_m M(m)$ かつ $m \succ_w M(w)$ であるような (m,w) を M の blocking pair と呼ぶ。blocking pair の存在しないマッチングを安定マッチングといい、安定マッチングを求める問題を安定結婚問題という。安定結婚問題の任意の例題に対して、安定マッチングが存在することは Gale と Shapley によって 1962 年に示されており、安定マッチングを $O(N^2)$ 時間で求めるアルゴリズム (Gale-Shapley アルゴリズム) も示されている。

安定結婚問題の現実世界での応用として、アメリカでは研修医を病院に割り当てる NRMP というマッチングシステムにこの問題が使われている。同様のシステムはカナダやスコットランドでも取り入れられており、日本でも 2004 年度の研修医配属から安定結婚問題が利用され始めた。

安定結婚問題の拡張として、希望リスト内に全員の名前を含まなくても良い不完全リストと、希望リスト内での同順位を許す同順位リストの二つの拡張が考えられるが、片方の拡張の下では、安定マッチングは全て同サイズであり、安定マッチングは多項式時間で求めることができる。ところが、これらの両方の拡張を同時に施すと、一つの例題に対して異なったサイズの安定マッチングが存在する可能性があり、その最大サイズの安定マッチングを見つける問題 (MAX SMTI) は APX 完全であることが知られている。MAX SMTI に対して、近似度 2 を達成するアルゴリズムの存在は自明である。近年、近似度 $2-c\frac{\log N}{N}$ (N は入力における男性の数、c は任意の正定数) のアルゴリズムが示された。本研究ではこのアルゴリズムを改良し、近似度 $2-c\frac{1}{N^{\frac{2}{3}}}$ (c は $c \leq \frac{1}{2\sqrt[3]{6}}$ を満たす正定数) を与えた。

10 グラフ上のゲームの必勝法

本研究では、チョンプとニムという、グラフ上で定式化できる二人ゲームについて、その必勝法を考察した。チョンプでは、最初に $m \times n$ の盤面状の長方形のチョコレート板が与えられる。左上の四角は毒チョコである。このチョコレート板を

交互に１つずつ食べていく。あるチョコを食べる際は、その右と下にある全てのチョコも食べなければならない。こうして、最後に毒チョコを食べてしまった方が負け、というゲームである。

このゲームは、先手必勝手順が存在することが証明されている。具体的な先手必勝手順は、$1\times n$, $2\times n$, $n\times n$ のチョコレート板に関しては発見されているが、それ以外の場合には知られていない。現段階では $3\times n$ のチョコレート板での先手必勝手順が研究されている。この研究の中で、必敗の盤面（「負け型」と呼ぶ）が膨大に列挙され、その中でいくつか法則が見つかっているものの、未だ先手必勝手順の発見には至っていないのが現状である。

チョンプにおいては、$m\times n$ のチョコレート板でチョコ (a,b) を食べる操作と、$n\times m$ のチョコレート板で四角 (b,a) を食べる操作とは等価である。この対称性に注目して、$3\times n$ のチョコレート板に限定せずに負け型を列挙し、法則を発見するという方法も考えられる。本研究では、計算機を用いて 9×9 までの全ての負け型（438 個）を列挙した。

また、チョンプに類似した、チョンプより簡単なゲームの必勝法から、チョンプの必勝法を導く方法が考えられる。そのようなゲームとして、ニムおよび木型のニムがあげられる。木型のニムは、木構造のグラフから、交互に１つの節点とその子孫を除いていき、根節点を除いた方が負け、というゲームである。ニムは、その木構造の分岐が根節点でのみ生じているものである。ニム、木型のニムについては、既に必勝法が知られている。

これらのゲームにおける根節点を、取ってはならない節点なので毒節点とおく。これらのゲームでは毒節点は根に一つだけあるが、本研究ではこれらのゲームを拡張し、毒節点の数と配置場所に制限を加えないものを扱った。この場合、毒節点を取れば即座に負ける場合と、毒節点を数回（これを「体力」と呼ぶ）までなら取ることができる場合とが考えられるが、本研究では、木型のニムの必勝法を応用することで、前者の必勝法を示した。後者においては、体力が多い方が必勝するということと、その具体的必勝法を示した。また、体力が同じ場合の必勝法も示した。

さらに、チョンプの拡張として、任意の場所に任意数の毒チョコが与えられるものが考えられる。この場合も、毒節点を複数持つ木型のニムと同様に、体力が多い方が必勝法を持つことを示した。体力が同じ場合は、右下のチョコが毒である場合は後手が、そうでない場合は先手が必勝法を持つことを示した。

11　論理回路の計算量の階層

論理回路の計算量とは、その論理関数を計算するのに必要な段数や素子数における最小値のことをいう。回路計算量における長年の研究の結果、様々な階層構造が証明されている。本研究ではクラス AC^0 というクラス内における階層構造を示した。クラス AC^0 とは、n 変数論理関数を計算する回路を作成するときに、入力制限のない AND、OR、NOT 素子を用いて定数段数、多項式サイズで実現可能な関数のクラスである。

この階層内において、線形サイズでは実現できないが多項式サイズでは実現できる関数の存在は最近まで示されていなかったが、昨年、$Size(s)$ では実現できないが $Size(s\log^{2+\varepsilon}s)$ で実現できる関数の存在が示された。しかし、これは存在を示しただけであり、具体的な関数を示したものではない。本研究では、パリティ関数を利用することにより、具体的な関数に対して上記の階層を示した。

12　家系図推定問題

進化系統樹とは、地球上の生物が共通の祖先から進化したと考えた時の、種間の進化的な関係を表現した木構造である。遺伝的な情報から進化系統樹を推定する方法に対する研究はさかんに行われてきた。また系統樹の一部に修正を加えたデータ構造を推定する研究も近年行われきている。

これに対し、家系図は進化系統樹をさらに詳しくしたものと考えることができる。進化系統樹をグラフで表現すれば有向木になるのに対し、家系図は入次数が 2 以下の非閉路的有向グラフとなる。本研究では、与えられた 2 節点間の遺伝的距離を満足する家系図を全て列挙する問題を考え、所望の家系図の全てが、節点数を増やすことなく一つ

の有向グラフで表現できることを示し、それを得る $O(n^3)$ 時間アルゴリズムを与えた。

13 通信遅延が大きな並列計算環境に対するタスクスケジュールのためのクラスタリングアルゴリズム

並列計算環境で効率よく計算を行うには、計算を構成する各タスク（部分計算）について、それを実行するプロセサと実行開始のタイミングを適切に調整することが重要である。各タスクを実行するプロセサと実行開始のタイミングを決定することはタスクスケジューリングとよばれ、これまでに多くの研究が行われている。これまでの研究のほとんどは、プロセサが密結合された並列計算環境を対象としており、プロセサがタスク処理に要する時間に比べ、プロセサ間通信の時間は十分に小さいと仮定している。

しかし、近年、PC クラスタなどプロセサ間の通信遅延の大きな並列計算環境の利用が広まっている。そこで本研究では、通信遅延の大きな並列計算環境において、高速な並列計算を実現するタスクスケジューリングを行うためのクラスタリングアルゴリズムについて考察した。

タスクの実行順序制約を規定するタスクグラフが与えられたときに、まず各プロセサに割り当てるタスクの集合を決定し（クラスタリング）、次に各プロセサ内でのタスクの実行開始時間を決定することによって、タスクスケジューリングを行うことができる。本研究では、タスクスケジューリングの第１段階であるクラスタリングのみを対象としている。

本研究では、まずクロスクラスタリングというクラスタリングのクラスを提案し、このクラス内に 1.5-近似スケジュールを導くクラスタリングが存在することを示した。さらに、タスクの複製を認めないという制約のもとでクロスクラスタリングを行う発見的アルゴリズムを提案し、提案するアルゴリズムが通信遅延の大きな並列計算環境において、効率的なタスクスケジュールを導くことをシミュレーションによって示した。

14 木ネットワークにおけるビザンチン故障耐性を有する自己安定辺彩色プロトコル

自己安定分散プロトコルは、計算機の故障によって分散システムがどのような状況に陥っても、故障が十分に長い間存在しなければ、いずれ正しい動作に復帰することを保証する分散システムである。つまり、自己安定分散システムは計算機の一時的な故障に対する高度な故障耐性を有する。

しかし、計算機の一部が断続的に故障する分散環境では、自己安定分散プロトコルの動作について何も保証できない。インターネットのような大規模な分散システムでは、故障が十分に長い間存在しないと仮定することは非現実的である。そのため、永久的な故障が存在する分散環境においても、正しい動作に復帰することを保証する自己安定分散システムの開発が重要である。

本研究では、永久故障としてビザンチン故障を対象とし、永久ビザンチン故障に対する故障耐性を有する木ネットワークの辺彩色プロトコルを設計した。このプロトコルでは、プロセスの並行性を決めるスケジューラとして、同時に動作するプロセスが１つである C デーモンを仮定している。このプロトコルは、木ネットワークの $\Delta + 1$-彩色（Δ は木の最大次数）を行うが、各正常プロセスは距離 2 以内にビザンチン故障プロセスが存在しなければ子への辺を正しく彩色して安定することが保証される。つまり、ビザンチン故障に対して、半径 2 の故障封じ込めを実現している。

また、色数を Δ に制限した場合は、故障封じ込め半径が $\Omega(\log n)$（n は木ネットワークのノード数）になることを証明した。さらに、同時に複数のプロセスの動作を許す D デーモンを仮定する場合は、故障封じ込め半径が $\Omega(n)$ になることを証明した。故障封じ込め半径に関するこれらの下界から、提案したプロトコルの色数とスケジューラに関する仮定が必要であることが示せた。

15 モバイルエージェントシステムのための自己安定基盤アルゴリズム

大規模・複雑化し、多様なダイナミクスを内包する分散環境において、効率的に正しく動作する分散システムの設計はますます困難になってきている。このようなダイナミクスを有する分散環境での分散システム設計の効果的なパラダイムとして、モバイルエージェントを活用した分散システム設計が有望視されている。ここでモバイルエージェントとは、ネットワークを移動しながら自律的に動作するプログラムのことである。

ダイナミクスへの高度な適応性を実現するには、分散システムの自己安定化が重要である。そこで本研究では、高度な適応性を有するモバイルエージェントシステムの開発の基盤となる、自己安定アルゴリズムの設計を行った。

まず、木ネットワークにおけるエージェントの自己安定巡回アルゴリズムを開発した。本研究では、n ノードからなる木ネットワークにおいて、n 個のモバイルエージェントが、各ノードに同時に 2 つ以上のエージェントが存在しないという制約の下でネットワークを巡回する問題を考察し、この問題に対する自己安定アルゴリズムを設計した。提案したアルゴリズムでは、各エージェントが木ネットワークの巡回に要する時間は $O(\Delta n)$（Δ は木の最大次数）である。さらに、この巡回時間がオーダ的に最適であることを示した。

次に、モバイルエージェント数を制御する自己安定アルゴリズムを開発した。モバイルエージェントを利用した分散システムでは、ネットワーク中のエージェント数が多いほど処理に要する時間が減少するが、システムの負荷は増加する。従って、ネットワーク中のエージェント数をネットワークの規模に対して適切に維持することが重要である。そこで本研究では、動的に変化するネットワークにおいて、エージェント数をノード数の一定割合に保つ問題について考察し、生態系パラダイムに基づいた手法を提案した。また、提案手法がエージェント数をノード数に対して所定の比に保つことをランダムネットワーク、スケールフリーネットワークなどのさまざまな種類のネットワークに対するシミュレーションによって示した。

研究業績一覧

学術論文

1. A. Uejima, H. Ito, and T. Tsukiji: "$\overline{C_7}$-coloring problem", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E87-A, No. 5, pp. 1243-1250, 2004 年 5 月.
   概要: *H-coloring problem* is a coloring problem with restrictions such that some pairs of colors cannot be used for adjacent vertices, where H is a graph representing the restrictions of colors. We deal with the case that H is the complement graph $\overline{C_{2p+1}}$ of a cycle of odd order $2p+1$. This paper presents the following results: (1) chordal graphs and internally maximal planar graphs are $\overline{C_{2p+1}}$-colorable if and only if they are p-colorable ($p \geq 2$), (2) $\overline{C_7}$-coloring problem on planar graphs is NP-complete, and (3) there exists a class that includes infinitely many $\overline{C_7}$-colorable but non-3-colorable planar graphs.

2. A. Uejima, and H. Ito: "Subdivision of the hierarchy of H-colorable graph classes by circulant graphs", CTW04 Workshop on Graphs and Combinatorial Optimization, pp. 232-236, 2004 年 5 月.
   概要: For any integer $p \geq 2$, p-colorable graphs are $\overline{C_{2p+1}}$-colorable and $\overline{C_{2p+1}}$-colorable graphs are $p+1$-colorable, where $\overline{C_{2p+1}}$ is the complement graph of a cycle of order $2p+1$. The converse statements are however incorrect. This paper presents that the above inclusion can be subdivided by a subset of circulant graphs $H(n,k)$ ($n, k \in \boldsymbol{N}$, $k \leq \lfloor n/2 \rfloor$). The subdivided hierarchy of inclusion contains the well-known inclusion of C_{2p+1}-colorable graphs. Moreover, we prove some NP-complete problems for planar $H(n,k)$-colorings, including the $\overline{C_5}$-coloring.

3. K. Iwama, and K. Yonezawa:

"The Orthogonal CNN Problem", Information Processing Letters, vol.90, no.3, pp.115–120, 2004 年 5 月.

概要: The online CNN Problem had no known competitive algorithms for a long time. Sitters, Stougie and de Paepe showed that there exists a competitive online algorithm for this problem. However, both their algorithm and analysis are quite complicated, and above all, their upper bound for the competitive ratio is 10^5. In this paper, we examine why this problem seems so difficult. To this end we introduce a nontrivial restriction, orthogonality, against this problem and show that it decreases the competitive ratio dramatically, down to at most 9.

4. 野口智史, 大下福仁, 増澤利光:
"通信遅延が大きな並列計算環境に対するタスクスケジューリングのためのクラスタリングアルゴリズム", 第 2 回先進的計算基盤システムシンポジウム論文集 (SACSIS 2004), pp.197-206, 2004 年 5 月.

概要: 近年, PC クラスタなどプロセッサ間の通信遅延の大きな並列計算環境が用いられている. 本論文では, 通信遅延の大きな並列計算環境において, 高速な並列計算を実現するタスクスケジューリングをおこなうためのクラスタリングアルゴリズムについて考察する. 本論文では, まずクロスクラスタリングというクラスタリングのクラスを提案し, このクラス内に 1.5-近似スケジュールを導くクラスタリングが存在することを示す. さらに, タスクの複製を認めないという制約のもとでクロスクラスタリングをおこなう発見的アルゴリズムを提案し, 提案するアルゴリズムが通信遅延の大きな並列計算環境において, 効率的なタスクスケジュールを導くことをシミュレーションによって示す.

5. Taisuke Izumi, Akinori Saitoh, Toshimitsu Masuzawa:
"Timed uniform consensus resilient to crash and timing faults", Proceedings of the International Conference on Dependable Systems and Networks (DSN 2004), pp.243-252, 2004 年 6 月.

概要: Δ-timed uniform consensus is a stronger variant of the traditional consensus and it satisfies the following additional property: The correct process terminates its execution within a constant time Δ (Δ-timeliness), and no two processes decide differently (Uniformity). In this paper, we consider the Δ-timed uniform consensus problem in presence of f_t crash processes and f_c timing-faulty processes. This paper proposes a Δ-timed uniform consensus algorithms. The proposed algorithm is adaptive in the following sense: It solves the Δ-timed uniform consensus when at least $f_t + 1$ correct processes exist in the system. If the system has less than f_t+1 correct processes, the algorithm cannot solve the Δ-timed uniform consensus. However, as long as $f_t + 1$ processes are non-crashed, the algorithm solves (non-timed) uniform consensus. We also investigate the maximum number of faulty processes that can be tolerated. We show that any Δ-timed uniform consensus algorithm tolerating up to f_t timing-faulty processes requires that the system has at least $f_t + 1$ correct processes. This impossibility result implies that the proposed algorithm attains the maximal resilience about the number of faulty processes. We also show that any Δ-timed uniform consensus algorithm tolerating up to f_t timing-faulty processes cannot solve the (non-timed) uniform consensus when the system has less than $f_t + 1$ non-crashed processes. This impossibility result implies that our algorithm attains the maximum adaptiveness.

6. Iwama, K.:
"Automated competitive analysis of online algorithms", Workshop on On-Line Algorithms (OLA 2004), 2004 年 7 月.

概要: The main objective of this paper is to

present a rather general framework for automated competitive analysis, i.e., for using computers to prove a competitive ratio of online algorithms. As an example, we use the Exchangeable Online Knapsack problem and prove an upper bound of 1.3334 for its competitive ratio using our system. There are two features: (i) Our system automatically generates different "states" of the game, the entire size of which is usually much larger than the size of the algorithm description. (ii) For claiming a concrete value for the competitive ratio, our system can use formula expression or does not have to depend on numerical analysis. For this purpose our system includes Mathematica as a part of the system.

7. Iwama, K., Miyazaki, S. and Okamoto, K.:
"A $(2 - c \log N/N)$-Approximation Algorithm for the Stable Marriage Problem", Proceedings of the 9th Scandinavian Workshop on Algorithm Theory (SWAT 2004), Lecture Notes in Computer Science 3111, pp. 349-361, 2004年7月.
概要: We propose an approximation algorithm for the problem of finding a maximum stable matching when both ties and unacceptable partners are allowed in preference lists. Our algorithm achieves the approximation ratio $2 - c\frac{\log N}{N}$ for an arbitrarily positive constant c, where N denotes the number of men in an input. This improves the trivial approximation ratio of two.

8. Iwama, K.:
"Worst-case upper bounds for kSAT", EATCS Bulletin, No. 82, pp. 61-71, 2004.
概要:

9. Hiro Ito, Kazuo Iwama, and Takeyuki Tamura:
"Imperfectness of Data for STS-Based Physical Mapping", IFIP World Computer Congress, pp. 279–292, 2004年8月.
概要: In the STS-based mapping, we are requested to obtain the correct order of probes in a DNA sequence from a given set of fragments or equivalently a hybridization matrix A. It is well-known that the problem is formulated as the combinatorial problem of obtaining a permutation of A's columns so that the resulting matrix has the consecutive-one property. If the data (the hybridization matrix) is error free and includes enough information, then the above column order determines the correct order of the probes uniquely. Unfortunately this is no longer true if the data include errors, which has been one of the popular research targets in computational biology. Even if there is no error, ambiguities in the probe order may still remain. This in fact happens by the lack of some information of the data, but almost no further investigation was made previously. In this paper, we define a measure of such imperfectness of the data as a minimum amount of additional fragments which are needed to fix the probe order uniquely. Several polynomial-time algorithms to compute such additional fragments of minimum cost are presented.

10. Tomokazu Imamura, Kazuo Iwama and Tatsuie Tsukiji:
"Approximated Vertex Cover for Graphs with Perfect Matchings", Proc. 10th Annual International Conference (COCOON 2004), pp.132–142, 2004年8月.
概要: Chen and Kanj considered the Vertex Cover problem for graphs with perfect matchings (VC-PM). They showed that: (i) There is a reduction from general Vertex Cover to VC-PM, which guarantees that if one can achieve an approximation factor of less than two for VC-PM, then one can do so for general Vertex Cover as well. (ii) There is an algorithm for VC-PM whose approximation factor is given as $1.069 + 0.069d$ where d is the average degree of the given graph. In this paper we improve

(ii). Namely we give a new VC-PM algorithm which greatly outperforms the above one and its approximation factor is roughly $2 - \frac{6.74}{d+6.28}$. Our algorithm also works for graphs with "large" matchings although its approximation factor is degenerated.

11. N. Doi, T. Horiyama, M. Nakanishi, and S. Kimura:
"An Optimization Method in Floating-point to Fixed-point Conversion using Positive and Negative Error Analysis and Sharing of Operations", Proc. the 12th Workshop on Synthesis And System Integration of Mixed Information Technologies (SASIMI 2004), pp.466–471, 2004 年 10 月.
概要:

12. Halldorsson, M., Iwama, K., Miyazaki, S. and Yanagisawa, H.:
"Randomized Approximation of the Stable Marriage Problem", Theoretical Computer Science, Vol. 325, No. 3, pp. 439-465, 2004 年 10 月.
概要: While the original stable marriage problem requires all participants to rank all members of the opposite sex in a strict order, two natural variations are to allow for incomplete preference lists and ties in the preferences. Either variation is polynomially solvable, but it has recently been shown to be NP-hard to find a maximum cardinality stable matching when both of the variations are allowed. It is easy to see that the size of any two stable matchings differ by at most a factor of two, and so, an approximation algorithm with a factor two is trivial. In this paper, we give a randomized approximation algorithm RandBrk and show that its expected approximation ratio is at most $10/7 (< 1.4286)$ for a restricted but still NP-hard case, where ties occur in only men's lists, each man writes at most one tie, and the length of ties is two. We also show that our analysis is nearly tight by giving a lower bound $32/23 (> 1.3913)$ for RandBrk. Furthermore, we show that these restrictions except for the last one can be removed without increasing the approximation ratio too much.

13. 野口智史, 大下福仁, 増澤利光:
"通信遅延が大きな並列計算環境に対するタスクスケジュールのためのクラスタリングアルゴリズム", 情報処理学会論文誌コンピューティングシステム, 第 45 巻, No.SIG11(ACS7), pp.257-268, 2004 年 10 月.
概要: 近年, PC クラスタなどプロセッサ間の通信遅延の大きな並列計算環境が用いられている. 本論文では, 通信遅延の大きな並列計算環境において, 高速な並列計算を実現するタスクスケジューリングをおこなうためのクラスタリングアルゴリズムについて考察する. 本論文では, まずクロスクラスタリングというクラスタリングのクラスを提案し, このクラス内に 1.5-近似スケジュールを導くクラスタリングが存在することを示す. さらに, タスクの複製を認めないという制約のもとでクロスクラスタリングをおこなう発見的アルゴリズムを提案し, 提案するアルゴリズムが通信遅延の大きな並列計算環境において, 効率的なタスクスケジュールを導くことをシミュレーションによって示す.

14. Taisuke Izumi, Toshimitsu Masuzawa:
"Synchronous condition-based consensus adapting to input-vector legality", Proceedings of the 18th International Symposium on Distributed Computing (DISC 2004), LNCS 3274, pp.16-29, 2004 年 10 月.
概要: This paper proposes a novel condition-based algorithm for the uniform consensus in synchronous systems. The proposed algorithm is *adaptive* in the sense that its execution time depends on actual difficulty of input vectors, *legality level*, which is newly formalized in this paper. On the assumption that majority of processes

are correct, the algorithm terminates within $\min\{f+2-l, t+1\}$ rounds if $l < f$, where f and t is the actual and the maximum numbers of faults respectively, and l is the legality level of input vectors. Moreover, the algorithm terminates in 1 round if $l \geq t$ and $f = 0$, and terminates within 2 rounds if $l \geq f$ holds. Compared with previous algorithms, for the case of $t < n/2$, the algorithm achieves the best time complexity in almost all situations.

15. Yoshihiro Nakaminami, Toshimitsu Masuzawa, Ted Herman:
"Self-stabilizing agent traversal on tree networks", IEICE Transactions on Information and Systems (Special Section on New Technologies and their Applications of the Internet), Vol. E87-D, No. 12, pp. 2773-2780, 2004年12月.
概要: This paper introduces the problem of n mobile agents that repeatedly visit all n nodes of a given network, subject to the constraint that no two agents can simultaneously occupy a node. This paper first presents a self-stabilizing phase-based protocol for a tree network on a synchronous model. The protocol realizes agent traversal with $O(\Delta n)$ time where n is the number of nodes and Δ is the maximum degree of any vertex in the communication network. The phase-based protocol can also be applied to an asynchronous model and a ring network. This paper also presents a self-stabilizing link-alternator-based protocol with agent traversal time of $O(\Delta n)$ for a tree network on an asynchronous model. The protocols are proved to be asymptotically optimal with respect to the agent traversal time.

16. Iwama, K., and Kawachi, A.:
"Approximated Two Choices in Randomized Load Balancing", Proceedings of the Fifteenth International Symposium on Algorithms and Computation (ISAAC2004), Lecture Notes in Computer Science 3341, p.545-557, 2004年12月.
概要: This paper studies the maximum load in the *approximated* d-choice balls-and-bins game where the current load of each bin is available only approximately. In the model of this game, we have r thresholds $T_1, ..., T_r$ $(0 < T_1 < \cdots < T_r)$ for an integer r (≥ 1). For each ball, we select d bins and put the ball into the bin of the lowest range, i.e., the bin of load i such that $T_k \leq i \leq T_{k+1} - 1$ and no other selected bin has height less than T_k. If there are two or more bins in the lowest range (i.e., their height is between T_k and $T_{k+1} - 1$), then we assume that those bins cannot be distinguished and so one of them is selected uniformly at random. We then estimate the maximum load for n balls and n bins in this game. In particular, when we put the r thresholds at a regular interval of an appropriate Δ, i.e., $T_r - T_{r-1} = \cdots = T_2 - T_1 = T_1 = \Delta$, the maximum load $L(r)$ is given as $(r + O(1)) \sqrt[r+1]{\frac{r+1}{(d-1)^r} \ln n / \ln\left(\frac{r+1}{(d-1)^r} \ln n\right)}$. The bound is also described as $L(\Delta) \leq \{(1+o(1)) \ln\ln n + O(1)\}\Delta / \ln((d-1)\Delta)$ using parameter Δ. Thus, if Δ is a constant, this bound matches the (tight) bound in the original d-choice model given by Azar et al., within a constant factor. The bound is also tight within a constant factor when $r = 1$.

17. Yusuke Sakurai, Fukuhito Ooshita, Toshimitsu Masuzawa:
"A self-stabilizing link-coloring protocol resilient to Byzantine faluts in tree networks", Proceedings of the 8th International Conference on Principles of Distributed Systems (OPODIS 2004), pp.196-206, 2004年12月.
概要: Self-stabilizing protocols can tolerate any type and any number of transient faults. But self-stabilizing protocols have no guarantee of their behavior against per-

manent faults. Thus, investigation concerning self-stabilizing protocols resilient to permanent faults is important. This paper proposes a self-stabilizing link-coloring protocol resilient to (permanent) Byzantine faults in tree networks. The protocol assumes the central daemon, and uses $\Delta + 1$ colors where Δ is the maximum degree in the network. This protocol guarantees that, for any nonfaulty process v, if v has no Byzantine ancestor with the distance of two or less and has no crash parent, v reaches its desired states within three rounds and never changes its states after that. Thus, it achieves fault containment with radius of two. Moreover, we prove that the containment radius becomes $\Omega(\log n)$ when we use only Δ colors, and prove that the containment radius becomes $\Omega(n)$ under the distributed daemon. These lower bound results prove necessity of $\Delta + 1$ colors and the central daemon to achieve fault containment with a constant radius.

18. Hiroyoshi Miwa and Hiro Ito:
"NA-edge-connectivity augmentation problems by adding edges", Journal of the Operations Reserch Society of Japan, Vol. 47, No. 4, pp. 224–243, 2004年.
概要: In a recent communication network, some mirror servers that provide the same service as an original server are often used. From the view of the network reliability, it is important that a client can access to at least one of the original or its mirror servers, even if some links or nodes fail. Therefore, it is necessary to design a network so that it ensures some independent routes between a client and a set of servers that provide the same service. When a communication network is modeled by a graph, the connectivity between a client and some mirror servers can be measured by NA(Node-to-Area)-edge(resp. vertex)-connectivity between a vertex and a vertex subset (an area), which is equal to the number of edge(resp. vertex)-independent paths between a vertex and an area. In this paper, we focus on the network design problem to increase the reliability of a current network by adding the smallest number of links. This problem can be formulated as the problem of augmenting a graph by adding the smallest number of new edges to meet NA-edge(vertex)-connectivity requirement. First, we prove the NP-completeness of the problem to determine whether a graph can be 1-NA-edge-connected by adding the given number or less of edges. Next, we show that the problem of augmenting a graph to be 2-NA-edge-connected by adding the smallest edges can be solved in polynomial time.

19. T. Imamura and K. Iwama:
"Approximating Vertex Cover on Dense Graphs", Proc. 16th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2005), pp. 582–589, 2005年1月.
概要: Although many problems in MAX-SNP admit a PTAS for dense graphs, that is not the case for Vertex Cover, which is MAX-SNP hard even for dense graphs. This paper presents a randomized approximation algorithm for Vertex Cover on dense graphs, i.e., graphs whose average degree d is $\Omega(n)$. (i) Our algorithm improves the best-known bound for the approximation factor by Karpinski and Zelikovsky. For example, our bound is $\frac{2}{1+\frac{d}{2\Delta}}$ for dense graphs such that $|E| \leq \Delta(n - \Delta)$ where Δ is the maximum degree. The improvement is especially large when $d \approx \Delta$; if $d \geq \frac{2}{3}\Delta$ for instance, our bound is at most 1.5 while the previous bound approaches to 2.0 as $\frac{n}{\Delta}$ increases. (ii) It achieves the same factor for a wider range of graphs, i.e., for the graphs whose Δ is $\Omega(n\frac{loglogn}{logn})$. (iii) It is probably optimal in the sense that if we can achieve a better approximation factor by $\delta > 0$ for the

above range of graphs, then we can achieve a factor of $2-\delta$ for general graphs.

20. Iwama, K., Kawachi, A., and Yamashita, S.:
"Quantum Sampling for Balanced Allocations", IEICE transactions on Information and Systems, Vol.E88-D No.1, p.47-52, 2005年1月.
概要: It is known that the original Grover Search (GS) can be modified to use a general value for the phase θ of the diffusion transform. Then, if the number of answers is relatively large, this modified GS can find one of the answers with probability one in a single iteration. However, such a quick and error-free GS can only be possible if we can initially adjust the value of θ correctly against the number of answers, and this seems very hard in usual occasions. A natural question now arises: Can we enjoy a merit even if GS is used without such an adjustment? In this paper, we give a positive answer using the balls-and-bins game in which the random sampling of bins is replaced by the quantum sampling, i.e., a single round of modified GS. It is shown that by using the quantum sampling: (i) The maximum load can be improved quadratically for the static model of the game and this improvement is optimal. (ii) That is also improved to $O(1)$ for the continuous model if we have a certain knowledge about the total number of balls in the bins after the system becomes stable.

21. Iwama, K., and Kawachi, A.:
"Compact Routing with Stretch Factor of Less Than Three", IEICE transactions on Information and Systems, Vol.E88-D No.1, p.39-46, 2005年1月.
概要: Cowen gave a universal compact routing algorithm with a stretch factor of three and table-size of $O(n^{2/3}\log^{4/3} n)$ based on a simple and practical model. (The table-size is later improved to $O(n^{1/2}\log^{3/2} n)$.) This paper considers, using the same model, how the necessary table-size differs if the stretch factor must be *less than* three. It is shown that: (i) There is a routing algorithm with a stretch factor of two whose table-size is $(n-\sqrt{n}+2)\log n$. (ii) There is a network for which any routing algorithm that follows the model and with a stretch factor of less than three needs a table-size of $(n-2\sqrt{n})\log n$ in at least one node. Thus, we can only reduce roughly an *additive* $\sqrt{n}\log n$ (i.e., $\sqrt{n}$ table-entries) from the trivial table-size of $n\log n$ which obviously enables shortest-path routing. Furthermore it turns out that we can reduce only an additive $\log n$ (i.e., only one table-entry) from the trivial $n\log n$ if we have to achieve a stretch factor of less than *two*. Thus the algorithm (i) is (roughly) tight both in its stretch factor and in its table-size.

22. Hiroshi Fujiwara and Kazuo Iwama:
"Average-Case Competitive Analyses for Ski-Rental Problems", Dagstuhl Seminar 05031 (Algorithms for Optimization with Incomplete Information), 2005年1月.
概要: Let s be the ratio of the cost for purchasing skis over the cost for renting them. Then the famous result for the ski-rental problem shows that skiers should buy their skis after renting them $(s-1)$ times, which gives us an optimal competitive ratio of $2-1/s$. In practice, however, it appears that many skiers buy their skis before this optimal point of time and also many skiers keep renting them forever. In this paper we show that this behavior of skiers is quite reasonable by using an *average-case competitive ratio*. For an exponential input distribution $f(t)=\lambda e^{-\lambda t}$, optimal strategies are (i) if $1/\lambda \le s$, then skiers should rent their skis forever and (ii) otherwise they should purchase them after renting approx-

imately $s^2\lambda$ $(< s)$ times. Thus average-case competitive analyses give us the result which differs from the worst-case competitive analysis and also differs from the traditional average cost analysis. Other distributions and related problems are also discussed.

23. Kazuo Iwama, Akinori Kawachi, Rudy Raymond. H. P. and Shigeru Yamashita:
"Robust Quantum Algorithms for Oracle Indentification", The 8th Workshop on Quantum Information Processing (QIP 2005), 2005 年 1 月.
概要: The oracle identification problem (OIP) was introduced by Ambainis et. al., which is given as a set S of M oracles and a hidden oracle f. Our task is to figure out which oracle in S is equal to the hidden f by doing queries to f. OIP includes several problems such as Grover Search as special cases. In this paper, we design *robust* algorithms, i.e., those which are tolerant against noisy oracles, for OIP. Our results include: (i) For any oracle set S such that $|S|$ is polynomial in N, $O(\sqrt{N})$ queries are enough to identify the hidden oracle, which is obviously optimal since this OIP includes Grover Search as a special case. (ii) For the case that $|S| \leq 2^{N^d} (d < 1)$, we design an algorithm whose query complexity is $O(\sqrt{N \log M / \log N})$ and matches the lower bound proved before. (iii) We can furthermore design a robust algorithm whose complexity changes smoothly between the complexity of (ii) and the complexity of recovering all information about the hidden oracle whose complexity is O(N) as showed by Buhrman et. al. Thus our new algorithms are not only robust but also their query complexities are even better than the previous noiseless case.

24. Taisuke Izumi, Toshimitsu Masuzawa:
"Timed uniform atomic broadcast in presence of crash and timing faults", IEICE Transactions on Information and Systems (Special issue on Foudations of Computer Science), Vol. E88-D, No. 1, pp.72-81, 2005 年 1 月.
概要: Δ-Timed Atomic Broadcast is the broadcast ensuring that all correct processes deliver the same messages in the same order, and that delivery latency of any message broadcast by any correct process is some predetermined time Δ or less. In this paper, we propose a Δ-timed atomic broadcast algorithm in a synchronous system where communication delay is bounded by a known constant d and processes suffer both crash faults and timing faults. The proposed algorithm can tolerate f_c crash faults and f_t timing faults as long as at least $f_t + 1$ processes are correct, and its maximum delivery latency Δ is $(2f' + 7)d$ where f' is the actual number of (crash or timing) faulty processes. That is, the algorithm attains the *early-delivery* in the sense that its delivery latency depends on the actual number of faults rather than the maximum number of faults that the algorithm can tolerate. Moreover, the algorithm has a distinct advantage of guaranteeing that timing-faulty processes also deliver the same messages in the same order as the correct processes (Uniformity). We also investigate the maximum number of faulty processes that can be tolerated. We show that no Δ-timed atomic broadcast algorithm can tolerate f_t timing faults, if at most f_t processes are correct. The impossibility result implies that the proposed algorithm achieves the maximum fault-resilience with respect to the number of faulty processes.

25. 宮崎修一:
"安定結婚問題", 電子情報通信学会会誌, Vol.88, No.3, pp. 195-199, 2005 年 3 月.
概要: 安定結婚問題は二部グラフにおけるマッチング問題の一種である．複数の男女が

おり，各人は異性を自分の好みで順序づけした希望リストを持っている．その希望リストに基づいて「安定性」を満たすマッチング (結婚) を求めるのが，安定結婚問題である．この問題は，アメリカの研修医配属への応用が有名であるが，近年日本の研修医配属でも利用し始められた．本稿では，安定結婚問題の基本的性質や応用例を紹介する．

26. Hiro Ito, Kazuo Iwama, Yasuo Okabe, and Takuya Yoshihiro:
"Single-backup-table schemes for shortest-path routing", Theoretical Computer Science, Vol. 333, pp. 347–353, 2005 年 3 月.
概要: For networks employing shortest-path routing, we introduce a new recovery scheme that needs only one extra backup routing table. By precomputing this backup table, the network recovers from any single link-failure immediately after the failure occurs. To compute the backup routing table for this scheme, we use the almost-linear-time algorithm to solve r, v-problem, which is a variation of the best swap problem, presented by Nardelli, et al. We further show that the same solution can be computed in exactly linear time if the underlying graph is unweighted.

27. Taisuke Izumi, Toshimitsu Masuzawa:
"An improved algorithm for adaptive condition-based consensus", Proceedings of the 12th Colloquium on Structural Information and Communication Complexity (SIROCCO 2005), 2005 年 5 月発表予定.
概要: *Condition-Based Approach* studies restrictions on the inputs of a distributed problem, called *conditions*, to circumvent several impossibility results. Especially, for the synchronous consensus problem, the relation between conditions and time complexity bounds has been studied. In our previous work, we introduced the adaptiveness on time complexity of the condition-based approach, and established the *adaptive* condition-based approach: It classifies all possible input vectors into the hierarchical sequence of conditions according to their difficulty called *legality level*. For such hierarchy, adaptive algorithms achieve time complexity depending on the legality level of input vectors. In this paper, we propose an improved version of the adaptive condition-based algorithms for synchronous consensus that achieves better time complexity than the previous one. On the assumption that majority of processes are correct, the proposed algorithm terminates within $\min\{f+2, t+1\}-l$ rounds if $l < f$, where f and t is the actual and the maximum numbers of faults respectively, and l is the legality level of input vectors. Moreover, the algorithm terminates in 1 round if $l \geq t$ and $f = 0$, and terminates within 2 rounds if $l \geq f$ holds. Compared with our previous algorithm, the proposed algorithm improves time complexity by one round in the case of $f = t$ and $l > f$.

28. Tomoko Suzuki, Fukuhito Ooshita, Taisuke Izumi, Toshimitsu Masuzawa:
"Self-adaptation of mobile agent population in dynamic networks: a biologically inspired approach", Short Paper, Proceedings of the 2nd IEEE International Conference on Autonomic Computing (ICAC-05), 2005 年 6 月発表予定.
概要: In mobile-agent-based systems, larger number of agents generally require shorter time to complete the whole task but consume more resources (e.g., processing power and network bandwidth). Therefore, it is indispensable to keep an appropriate number of agents for its application. In this paper, we consider the mobile agent population control problem in dynamic networks; it requires to adapt the number of agents to a constant fraction of the current network size. We propose an algorithm inspired by a biological paradigm and show by simula-

tions that the proposed algorithm realizes self-adaptation of mobile agent population in dynamic networks.

29. Y. Hanatani, T. Horiyama, and K. Iwama: "Hajós Calculus on Planar Graphs", Proceedings of the 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, (掲載予定).
概要: The Hajós calculus is a nondeterministic procedure which generates the class of non-3-colorable graphs. If all non-3-colorable graphs can be constructed in polynomial steps by the calculus, NP = co-NP holds. Up to date, however, it remains open whether there exists a family of graphs that can be generated in polynomial steps. To attack this problem, we propose two graph calculi $\mathcal{PHC}$ and $\mathcal{PHC}^*$ that generate non-3-colorable planar graphs, where intermediate graphs in the calculi are also restricted to be planar. Then we prove that $\mathcal{PHC}$ and $\mathcal{PHC}^*$ are *sound* and *complete*. We also show that $\mathcal{PHC}^*$ can polynomially simulate $\mathcal{PHC}$.

30. H. Fujiwara, K. Iwama: "Average-Case Competitive Analyses for Ski-Rental Problems", Algorithmica, (掲載予定).
概要: Let s be the ratio of the cost for purchasing skis over the cost for renting them. Then the famous result for the ski-rental problem shows that skiers should buy their skis after renting them $(s-1)$ times, which gives us an optimal competitive ratio of $2-\frac{1}{s}$. In practice, however, it appears that many skiers buy their skis before this optimal point of time and also many skiers keep renting them forever. In this paper we show that these behaviors of skiers are quite reasonable by using an *average-case competitive ratio*. For an exponential input distribution $f(t)=\lambda e^{-\lambda t}$, optimal strategies are (i) if $\frac{1}{\lambda} \leq s$, then skiers should rent their skis forever and (ii) otherwise should purchase them after renting approximately $s^2\lambda$ $(< s)$ times. Thus average-case competitive analyses give us the result which differs from the worst-case competitive analysis and also differs from the traditional average cost analysis. Other distributions and related problems are also discussed.

研究会等

1. 岡本和也, 宮崎修一, 岩間一雄:
"局所探索法による安定結婚問題の近似", 信学技報 COMP2004-8 (電子情報通信学会コンピュテーション研究会), Vol.104, No.16, pp.53-60, 2004 年 4 月.
概要: 安定結婚問題の例題では、各個人の希望リストは異性全員を含み、完全に順位付けされている必要がある。しかし、実世界での応用を考えると、ペアになりたくない相手は希望リストに書かない不完全リストや、好みが同じ程度の人は優劣をつけなくて良い同順位リストという 2 つの自然な拡張が考えられる。どちらか一方の拡張のみを許した問題は多項式時間で解くことができるが、両方の拡張を許した場合、最大サイズの安定マッチングを見つける問題は NP 困難になることが知られている。任意の 2 つの安定マッチングのサイズは最大でも 2 倍しか異ならないということは簡単にわかるため、近似度が 2 の近似アルゴリズムは自明である。2 よりも良い近似度を実現する近似アルゴリズムを与える結果はいくつか知られているが、それらは、例えば同順位の長さや出現数などの制限を加えられた下でのものだけである。現在まで一般的な入力に対し、近似度が 2 未満となる近似アルゴリズムは知られていない。本論文では、一般的な例題に対し、近似度が 2 未満となる非自明な結果を初めて示した。我々のアルゴリズムの近似度は $2-c\frac{\log N}{N}$ である。(ここで、c は任意の正定数で、N は入力中の男性の数である。)

2. Taisuke Izumi, Akinori Saitoh, Toshimitsu Masuzawa:

"Timed uniform consensus protocol tolerating crash and timing faults", 電子情報通信学会技術研究報告 DC2004-7, Vol. 104, No. 13, pp.33-38, 2004 年 4 月.

概要: Δ-timed uniform consensus is a stronger variant of the traditional consensus and it satisfies the following additional property: The correct process terminates its execution within a constant time Δ (Δ-timeliness), and no two processes decide differently (Uniformity). In this paper, we consider the Δ-timed uniform consensus problem in presence of f_t crash processes and f_c timing-faulty processes. This paper proposes a Δ-timed uniform consensus algorithms. The proposed algorithm is adaptive in the following sense: It solves the Δ-timed uniform consensus when at least $f_t + 1$ correct processes exist in the system. If the system has less than $f_t + 1$ correct processes, the algorithm cannot solve the Δ-timed uniform consensus. However, as long as $f_t + 1$ processes are alive, the algorithm solves (non-timed) uniform consensus. We also investigate the maximum number of faulty processes that can be tolerated. We show that any Δ-timed uniform consensus algorithm tolerating up to f_t timing-faulty processes requires that the system has at least $f_t + 1$ correct processes. This impossibility result implies that the proposed algorithm attains the maximal resilience about the number of faulty processes. We also show that any Δ-timed uniform consensus algorithm tolerating up to f_t timing-faulty processes cannot solve the (non-timed) uniform consensus when the system has less than $f_t + 1$ non-crashed processes. This impossibility result implies that our algorithm attains the maximum adaptiveness.

3. 中塚裕之, 堀山貴史, 岩間一雄, :
"逆算法に基づく詰将棋の列挙", 信学技報 COMP2004-20 (電子情報通信学会コンピュテーション研究会), Vol.104, pp.11-18, 2004 年 6 月.

概要: 近年の計算機の高速化や大容量化、洗練されたアルゴリズム設計法の発展により、与えられた条件を満たす解を 1 つだけでなくすべて列挙することが、実用上要請されるようになってきている。本研究では、逆算法による詰将棋の列挙アルゴリズムを提案する。従来手法では、詰将棋となる可能性のある局面を数え挙げ、これを順に詰将棋解答プログラムに解かせて それぞれが詰将棋として成立していることを確認しているため、実行時間が長くなりがちである。本手法では、逆算法により詰め手数の少ないものから順に詰将棋を列挙することで、詰将棋解答プログラムを用いることなく、与えられた条件下で可能な詰将棋を高速に列挙することができる。また、提案アルゴリズムを C 言語で実装し、桂図式等の複数の条件において列挙を行う。生成可能なものをすべて数え挙げられるため、例えば桂図式は最長手数が 9 手である等、各図式の最長手数を証明したことになる。

4. 河内亮周, 山下茂, 岩間一雄:
"オラクル同定問題に対する頑健な量子アルゴリズム", 情報処理学会 アルゴリズム研究会, 情処研報, 2004-AL-96, pp.1–8, 2004 年 7 月.

概要: オラクル同定問題とは n ビット入力 1 ビット出力のオラクルの集合 $S = \{f_1, ..., f_M\}$ と S に属する未知のオラクル f_i が与えられたとき, 未知のオラクル f_i を S の中から同定する問題であり, 数多くの問題の一般化になっている. 本稿では, 与えられた未知のオラクルクエリーの結果が 正しい値と誤った値が重ね合わせ状態として出力される場合の オラクル同定問題 (但し, 誤った計算結果が得られる確率は 1/2 より小さい定数確率, 例えば 1/10 以下とする.) に対して以下を示す. (i) 与えられたオラクル集合のサイズが $N = 2^n$ の場合 (すなわち $M = N$.), エラー付きオラクル同定問題をクエリー回数 $O(\sqrt{N})$ で少なくとも 定数確率で解く量子アルゴリズムが構成できる. (ii) 与えられたオラクル集合のサイズが N の場合, 各

$x \in \{0,1\}^n$ で $f_i(x) = 1$ を満たす i の数に関するパラメータ K に関して ある条件を満たすとき，エラー付きオラクル同定問題を クエリー回数 $O(\sqrt{N/K})$ で 少なくとも定数確率で解く量子アルゴリズムが構成できる．

5. 川原 純，堀山貴史，岩間一雄:
“オンラインアルゴリズムの競合比証明の自動化について”, 2004 年夏の LA シンポジウム, pp.22.1–22.4, 2004 年 7 月.
概要: 種々のオンライン問題では、オンラインアルゴリズムを設計し、 競合比を計算するが、しばしば場合分けが膨大な数に及ぶことがある。今回はそのような問題の代表としてオンラインナップザック問題を考える。 オンラインナップザック問題はプレイヤはアイテムが一つずつ順番に与えられ、 そのたびにそのアイテムをナップザックの中に入れるか捨てるかを決める オンライン問題である。この問題の競合比上限を証明するとき、 アイテムのサイズによる場合分けが 20 種類以上にも及ぶことが分かった [1]。 そこで、この場合分けを計算機を用いて自動的に生成し、競合比の証明を行う。 本稿では交換可能オンラインナップザック問題 (EOK) での $k = 2$ の場合の上限が 1.3334 であることを計算機を用いて証明を行った。

6. Xin Han, Kazuo Iwama. Guochuan Zhang:
“On-line Removable Square Packing”, 夏の LA シンポジウム, 2004 年 7 月.
概要: In this paper, we consider an on-line square packing problem: Given a list of squares with side length of at most 1, we are asked to pack a subset of them, in an on-line manner and without any overlap, into a unit square bin so that the packed area (the total area of squares packed) is as large as possible. We assume that removal is allowed. It means that a packed square can be removed from the square bin. However, once a square is rejected or removed it will never been considered again. We first show a lower bound of 2.618 for any on-line algorithm. Then we propose an on-line algorithm based on partitioning the square bin into bricks and show a competitive ratio of 3. As a byproduct it is proved that any list of squares with total area no more than 1/3 can be on-line packed in a unit square, which improves the previous best known result by Januszewski and Lassak.

7. Taisuke Izumi, Toshimitsu Masuzawa:
“Synchronous condition-based consensus algorithm adapting to input-vector legality”, 電子情報通信学会技術研究報告 COMP2004-31, Vol. 104, No. 314, pp.41-48, 2004 年 9 月.
概要: This paper proposes a novel condition-based algorithm for the uniform consensus in synchronous systems. The proposed algorithm is *adaptive* in the sense that its execution time depends on actual difficulty of input vectors, *legality level*, which is newly formalized in this paper. On the assumption that majority of processes are correct, the algorithm terminates within $\min\{f+2-l, t+1\}$ rounds if $l < f$, where f and t is the actual and the maximum numbers of faults respectively, and l is the legality level of input vectors. Moreover, the algorithm terminates in 1 round if $l \geq t$ and $f = 0$, and terminates within 2 rounds if $l \geq f$ holds. Compared with previous algorithms, for the case of $t < n/2$, the algorithm achieves the best time complexity in almost all situations.

8. 鈴木朋子, 泉泰介, 大下福仁, 増澤利光:
“動的ネットワークにおける生態系パラダイムに基づくモバイルエージェント数制御”, 情報処理学会数理モデル化と問題解決研究会 2004-MPS-52 (17) 資料, Vol.2004, No.130, pp.65-68, 2004 年 12 月.
概要: 分散システムの効果的な実現法として，モバイルエージェントを利用した設計法への期待が高まっている．モバイルエージェントを利用した分散システムでは，ネットワーク中の　エージェント数が多いほど処理に要す

る時間が減少するが，システムの負荷は増加する．従って，ネットワーク中のエージェント数をネットワークの規模に対して適切に設定することが重要である．本研究では，動的に変化するネットワークにおいて，エージェント数をノード数の一定割合に保つ問題について考察し，生態系パラダイムに基づいた手法を提案する．また，提案手法がエージェント数をノード数に対して所定の比に保つことをシミュレーションによって示す．

9. 田村武幸, 伊藤大雄, 岩間一雄:
“遺伝的な距離に基づいた家系図推定問題”, 電子情報通信学会 コンピュテーション研究会, 信学技報 Vol.104, No.642, pp33-39, 2005 年 1 月.
概要: 進化系統樹とは地球上の生物が、共通の祖先から進化したと考えた時の、種間の進化的な関係を表現した木構造である。遺伝的な情報から進化系統樹を推定する方法に対する研究はさかんに行われてきた。また系統樹の一部に修正を加えたデータ構造を推定する研究も近年行われきている。これに対し、家系図は進化系統樹をさらに詳しくしたものと考えることができる。進化系統樹をグラフで表現すれば有向木になるのに対し、家系図は入次数が 2 以下の非閉路的有向グラフとなる。本稿では、与えられた 2 節点間の遺伝的距離を満足する家系図を全て列挙する問題を考え、所望の家系図の全てが、節点数を増やすことなく一つの有向グラフで表現できることを示し、それを得る $O(n^3)$ 時間アルゴリズムを与える。

10. Yoichi Hanatani, Takashi Horiyama, Kazuo Iwama:
“Hajós Calculus on Planar Graphs”, 冬の LA シンポジウム, 2005 年 1 月.
概要: The Hajós calculus is a nondeterministic procedure which generates the class of non-3-colorable graphs. Unless NP $\neq$ co-NP, there must exist graphs which need exponential steps to be constructed in the Hajós calculus, however it is not known. In this paper, we propose new systems of graph calculus which generate the class of non-3-colorable planar graphs and show its upper bound.

11. 添田祐司, 泉泰介, 増澤利光:
“分散環境における順位つき資源への部分探索法の提案”, 情報処理学会マルチメディア通信と分散処理研究会資料, 2005 年 3 月 発表予定.
概要: 分散システム内に分散配置された資源の検索にかかるコストを小さくする方法 として部分検索法が提案されている．部分検索法とは，検索条件を満たす資源すべてではなく，その部分集合を検索結果とする手法である．しかし，既知の部分検索法では，利用者の要求に対して検索結果の精度が保証されていない．本稿では，順位つき資源に対して，利用者が得る検索結果の精度を保証する部分検索法を定式化する．また，効率のよい部分検索法を実現する方法として，各サーバが資源を，その順位に基づく保持確率で保持する確率的配置法を提案する．確率的配置法において，順位の高い資源ほど保持確率を高くすることで小さい検索コストを実現できることを示す．また，保持確率関数が与えられたとき，保持確率関数をステップ型の関数に変換することで，検索にかかるコストを悪化させることなく，順位の変動等によるシステム更新にかかるコストを改善できることを示す．

C10: 情報基盤アルゴリズムとしてのメタヒューリスティクスの研究

茨木 俊秀 † 柳浦 睦憲 ‡ 野々部 宏司 ‡ 巳波 弘佳 † 藤重 悟 §

† 関西学院大学 理工学部 情報科学科
〒 669-1337 兵庫県三田市学園 2-1
{ibaraki,miwa}@ksc.kwansei.ac.jp

‡ 京都大学 大学院 情報学研究科
〒 606-8501 京都市左京区吉田本町
{nonobe,yagiura}@i.kyoto-u.ac.jp

§ 京都大学 数理解析研究所
〒 606-8502 京都市左京区北白川追分町
fujishig@kurims.kyoto-u.ac.jp

1 はじめに

現在社会は、情報と通信技術に支えられた高度情報化社会と呼ばれているが、さらに成熟を加えて、知識社会へ変貌していくと言われている。そのためには、数々の課題を解決し、克服していかねばならないが、その過程で生ずる多くの問題が、数理的にはいわゆる組合せ問題、組合せ最適化問題の形に記述されることから、それらの解決を図るためのアルゴリズム研究が求められている。

我々の研究グループは、

1. 社会のさまざまな現象を数理的にモデル化する研究、
2. モデル化された問題を解決するためのアルゴリズムの研究、
3. 効果的なアルゴリズムを開発するための理論的基礎研究,

を行っている。第 1 のタイプの研究は、巳波が中心になって進めており、第 2 のタイプは柳浦と野々部が中心、第 3 のタイプは藤重が主に担当している。茨木はこのグループの研究総括を担当しているが、主に第 2 のタイプの研究に参加している。

多くの組合せ問題あるいは組合せ最適化問題は、計算的には困難な問題であって、理論的には NP 完全問題あるいは NP 困難問題のクラスに属する。これらの問題を現実的な意味で解決するには、効果的なアルゴリズムを可能にする数学的構造を見つけ出し、そのような問題へのモデル化を行うか、厳密な最適解の導出を目指すのではなく、良質の近似解を高速に求めるという目標に切り替えて、そのための近似アルゴリズムを開発する、という二つのアプローチが考えられる。近似アルゴリズムの研究は、近年きわめて盛んになっているが、このグループでは、メタヒューリスティクスの枠組みで、局所探索に立脚した種々のアルゴリズムに重心をおき、実用的な利用に耐えるようなアルゴリズムの開発を行ってきた。

本報告では、今年度に得られた研究成果を、上記のタイプ 2、タイプ 1、およびタイプ 3 の順に述べる。第 2〜4 章がそれぞれの内容である。

2 メタヒューリスティクスの枠組みに基づくアルゴリズムの開発

本年度は具体的な対象として、主に、時間枠制約つき配送計画問題、2 次元パッキング問題、多資源一般化割当問題、カッティングストック問題に対する研究を進めた。配送計画問題に対しては、客間の移動に要する時間が時刻に応じて変化する問題を考え、近似解法の提案を行った。これにより、朝や夕方に道路が混雑するといった、より現実的な状況にも対応可能となる。また、時間枠制約に対するペナルティを凸に限定することで、一般性をさほど損なうことなく大幅な高速化に成功した。カッティングストック問題についても、これまで開発を進めてきたソルバーにおいて新しい近傍操作を導入するとともに、ボトルネックとなっていた LP の反復計算の高速化に成功し、大幅に性能を改善することに成功した。

以下ではとくに、時刻依存配送計画問題に関する研究成果について報告する。

2.1 時刻依存配送計画問題に対する反復局所探索法

配送計画問題は, 様々な制約条件の下で, 複数の車両を用いて全ての客をちょうど 1 回ずつ訪問するような経路の中で, コストが最小のものを求める問題である [4]. この問題は NP 困難であるため, 現実的な方法として種々の近似解法が提案されている. 通常, 制約条件として各車両の容量制約と時間枠制約が取り扱われる. 容量制約とは, 客の要求量の総和が車両の容量を越えてはいけないというもので, 時間枠制約とは, 客が指定する時間枠内にサービスを開始しなければならないというものである. いずれの制約も, 容量制約のみを課した問題は分割問題を, 時間枠制約のみを課した問題はスケジューリング問題を特殊な場合として含むことから, 一方の制約のみを課した問題に対する実行可能解の存在の判定がすでに NP 完全である [1]. この点を克服する方法の 1 つとして, これらの制約を考慮制約として扱い, 制約の違反量に応じたコストを付加した目的関数を最小化するという方針がとられている [2].

本研究では, [2] の拡張として, 移動時間に時刻依存性を許したモデルを考案する. 従来の配送計画問題では, 移動時間は定数として与えられるが, 現実には, たとえば朝の通勤ラッシュなどのように時刻によって大きく変動する. そこで移動時間を移動開始時刻の関数として扱うモデルを考え, 局所探索法に基づく 1 つの近似解法を提案する.

2.2 問題定義

節点集合 $V = \{0, 1, \ldots, n\}$ と枝集合 $E = \{(i, j) \mid i, j \in V, i \neq j\}$ をもつ完全有向グラフ $G = (V, E)$ と車両集合 $M = \{1, 2, \ldots, m\}$ を考える. ここで節点 0 はデポと呼ばれる特殊な節点で, 各車両はデポから出発しデポに帰還しなければならない. また, 他の節点はサービスを受ける客を表す. 各客は 1 台の車両によってただ 1 度だけ訪問される.

客 $i \in V$, 車両 $k \in M$, 枝 $(i, j) \in E$ には以下のデータが与えられる.

- 各 $i \in V$ のサービス要求量 a_i (≥ 0), およびサービス開始時刻 t に対する時間枠コスト関数 $p_i(t)$ (≥ 0).
- 車両 k の容量 u_k (≥ 0).
- 枝 (i, j) の移動開始時刻 t に対する移動時間関数 $q_{ij}(t)$ (≥ 0) と距離 d_{ij}.

時間枠コスト関数 p_i と移動時間関数 q_{ij} は共に区分線形関数とし, また, q_{ij} は FIFO, すなわち条件 $t_1 \leq t_2 \Longrightarrow t_1 + q_{ij}(t_1) \leq t_2 + q_{ij}(t_2)$ を満たすものとする. 区分線形関数の各区分の情報は入力データとして明示的に与えられる.

ここで, 車両 k が訪問する客数を n_k, 車両 k のルート内の客の順列を $\sigma_k = (\sigma_k(1), \sigma_k(2), \ldots, \sigma_k(n_k))$ と記し, 全車両のルートを $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_m)$ で表す. なお, 各車両はデポを出発しデポに帰還するため, $\sigma_k(0) = \sigma_k(n_k + 1) = 0$ と定義する. さらに, s_i を客 i のサービス開始時刻, s^{a}_k を車両 k がデポに帰還する時刻, t_i を客 i を出発する時刻, t^{l}_k を車両 k がデポを出発する時刻とし, $\boldsymbol{s} = (s_1, s_2, \ldots, s_n, s^{\mathrm{a}}_1, s^{\mathrm{a}}_2, \ldots, s^{\mathrm{a}}_m)$, $\boldsymbol{t} = (t_1, t_2, \ldots, t_n, t^{\mathrm{l}}_1, t^{\mathrm{l}}_2, \ldots, t^{\mathrm{l}}_m)$, とする. 以上を用いて, 配送計画は $(\boldsymbol{\sigma}, \boldsymbol{s}, \boldsymbol{t})$ で与えらる.

また, 簡単のために曖昧でない場合は, $p^k_h(t) = p_{\sigma_k(h)}(t)$, $q^k_h(t) = q_{\sigma_k(h),\sigma_k(h+1)}(t)$, $s_0 = s^{\mathrm{a}}_k$, $t_0 = t^{\mathrm{l}}_k$ と記す. 車両 k の時間枠コスト, 移動時間, 移動距離, 容量超過量はそれぞれ

$$
\begin{aligned}
p^k_{\mathrm{sum}}(\sigma_k, \boldsymbol{s}) &= \sum_{h=1}^{n_k+1} p^k_h(s_{\sigma_k(h)}) \\
q^k_{\mathrm{sum}}(\sigma_k, \boldsymbol{t}) &= \sum_{h=0}^{n_k} q^k_h(t_{\sigma_k(h)}) \\
d^k_{\mathrm{sum}}(\sigma_k) &= \sum_{h=0}^{n_k} d_{\sigma_k(h),\sigma_k(h+1)} \\
a^k_{\mathrm{sum}}(\sigma_k) &= \max\left\{0, \sum_{h=1}^{n_k} a_{\sigma_k(h)} - u_k\right\}
\end{aligned}
$$

と表される. ルートを $\boldsymbol{\sigma}$ としたとき, $y_{ik}(\boldsymbol{\sigma}) \in \{0, 1\}, i \in V, k \in M$ を車両 k が客 i をサービスするなら $y_{ik}(\boldsymbol{\sigma}) = 1$, そうでないなら $y_{ik}(\boldsymbol{\sigma}) = 0$ と定義する. また, $cost(\sigma_k, \boldsymbol{s}, \boldsymbol{t}) = p^k_{\mathrm{sum}}(\sigma_k, \boldsymbol{s}) + q^k_{\mathrm{sum}}(\sigma_k, \boldsymbol{t}) + d^k_{\mathrm{sum}}(\sigma_k) + a^k_{\mathrm{sum}}(\sigma_k)$ とおく. 以上

より, 時間依存配送計画問題は以下のように定式化できる.

$$
\begin{aligned}
\min \quad & \sum_{k=1}^{m} cost(\sigma_k, \boldsymbol{s}, \boldsymbol{t}) \\
\text{s.t.} \quad & \sum_{k \in M} y_{ik}(\boldsymbol{\sigma}) = 1, \qquad i \in V \setminus \{0\} \\
& s_{\sigma_k(h)} \le t_{\sigma_k(h)}, \quad k \in M, h = 1, 2, \ldots, n_k \\
& t_{\sigma_k(h)} + q_h^k(t_{\sigma_k(h)}) \le s_{\sigma_k(h+1)}, \\
& \qquad\qquad k \in M, h = 0, 1, \ldots, n_k \\
& t_k^1 \ge 0, \qquad\qquad k \in M.
\end{aligned}
$$

上の定式化から分かるように, 全車両のルート $\boldsymbol{\sigma}$ が決定しても $\boldsymbol{s}$ と $\boldsymbol{t}$ が未定なために目的関数の値はまだ分からない. しかし, 2.3 節で述べるように, $\boldsymbol{\sigma}$ が与えられると, $\boldsymbol{s}$ と $\boldsymbol{t}$ は最適に求めることが可能である. 本研究では, $(\boldsymbol{\sigma}, \boldsymbol{s}, \boldsymbol{t})$ ではなく $\boldsymbol{\sigma}$ を 2.4 節で述べる局所探索法で探索する.

2.3 最適スケジュール決定問題

本研究では, 車両のルート $\boldsymbol{\sigma}$ を 2.4 節で述べる局所探索法で探索するが, 車両のルート $\boldsymbol{\sigma}$ が決まっても, さらに各客でのサービス開始時刻と移動開始時刻を最適化する問題を解かなければならない. この問題は車両ごとに独立である. 車両 k に対する最適スケジュール決定問題は,

$$
\begin{aligned}
\min \quad & p_{\mathrm{sum}}^k(\sigma_k, \boldsymbol{s}) + q_{\mathrm{sum}}^k(\sigma_k, \boldsymbol{t}) \\
\text{s.t.} \quad & s_{\sigma_k(h)} \le t_{\sigma_k(h)}, \qquad h = 1, 2, \ldots, n_k \\
& t_{\sigma_k(h)} + q_h^k(t_{\sigma_k(h)}) \le s_{\sigma_k(h+1)}, \\
& \qquad\qquad h = 0, 1, \ldots, n_k.
\end{aligned}
$$

と定義される. この問題は動的計画法により効率的に解くことができる. 以下にその概略を示す.

まず, 前向きコスト最小関数 $f_h^k(t)$ を

> 車両 k が時刻 t 以前に客 $\sigma_k(h)$ のサービスを行うとして, それ以前の客 $\sigma_k(0), \sigma_k(1), \ldots, \sigma_k(h)$ をすべてサービスするのにかかる時間枠コストと移動時間の総和の最小値

と定義する. このとき, $f_h^k(t)$ は漸化式

$$
\begin{aligned}
f_0^k(t) &= \begin{cases} +\infty, & t < 0 \\ 0, & t \ge 0 \end{cases} \\
f_h^k(t) &= \min_{s \le t} \left\{ p_h^k(s) + g_h^k(s) \right\} \\
& \qquad 1 \le h \le n_k + 1, \ -\infty < t < +\infty
\end{aligned}
$$

によって計算できる. ただし

$$
g_h^k(s) = \min_{t' : t' + q_{h-1}^k(t') \le s} \{ f_{h-1}^k(t') + q_{h-1}^k(t') \}
$$

である. 漸化式中の s と t' はそれぞれ, 客 $\sigma_k(h)$ のサービス開始時刻と客 $\sigma_k(h-1)$ からの出発時刻である. σ_k の時間枠コストと移動時間の総和の最小値は $\min_t f_{n_k+1}^k(t)$ によって得られることは定義から明らかである.

次に $f_1^k, f_2^k, \ldots, f_{n_k+1}^k$ を順に求める計算時間について概略を述べる. $\delta(\cdot)$ で区分線形関数の区分数を表すものとする. このとき

$$
\delta(f_h^k) \le \delta(p_h^k) + \delta(f_{h-1}^k) + \delta(q_h^k)
$$

が成り立つ. ここで, $\Delta_k = \sum_{h=0}^{n_k} \left(\delta(p_h^k) + \delta(q_h^k) \right)$ とおくと, $\delta(f_h^k) = O(\Delta_k)$ となる. また, f_{h-1}^k から f_h^k を求める計算時間は

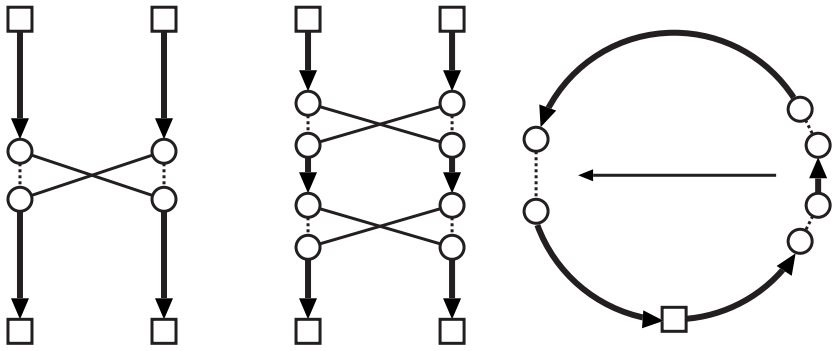
$$
O(\delta(p_h^k) + \delta(f_{h-1}^k) + \delta(q_h^k)) = O(\Delta_k)
$$

である. したがって $f_1^k, f_2^k, \ldots, f_{n_k+1}^k$ を計算し, $\min_t f_{n_k+1}^k(t)$ を求めるのは $O(n_k \Delta_k)$ 時間で可能である.

なお, 従来のモデル [2] でも, 与えられたルートからそのコストを求める必要があったが, この最適スケジュール決定問題はその問題の拡張となっている. また, このアルゴリズムは従来の問題に対しては同じ計算オーダーとなる.

2.4 局所探索法

本研究では, 車両のルート $\boldsymbol{\sigma}$ を局所探索法 (LS) を用いて探索する. 局所探索法とは, 現在の解 $\boldsymbol{\sigma}$ の近傍内に $\boldsymbol{\sigma}$ より良い解があればそれに置き換える, という操作を反復するものである.



(a) 2-opt* (b) クロス交換 (c) ルート内挿入

図 2.1: 近傍操作 (太線はパスを表す)

2.5 近傍

本研究では近傍として, 2-opt* 近傍, クロス交換近傍, およびルート内挿入近傍の 3 つを組合せて用いる. 図 2.1 は, これらの近傍を表している.

まず 2-opt* 近傍であるが, これは, 異なる 2 本のルートそれぞれを前半と後半の 2 つのパスに分け, 後半のパスを交換することにより得られる解集合である (図 2.1 (a)). クロス交換近傍は, 異なる 2 つのルートそれぞれからパスを選び, それらを互いに交換することによって得られる解集合である (図 2.1 (b)). 最後にルート内挿入近傍とは, ルート内の部分パスを同一ルートの他の位置へ挿入することによって得られる解集合である (図 2.1 (c)).

2.6 反復局所探索法

本研究では, 局所探索法を基本動作とする反復局所探索法 (ILS) を用いている. 通常, 局所探索法を 1 回適用しただけでは, 精度の良い解が得られないので, 本研究では, メタ戦略の 1 つである反復局所探索法を用いた. 反復局所探索法とは, 局所探索法で得られた局所的最適解にランダムな変形を施したものを初期解として局所探索法を行う, という操作を反復するものである. これを手続きとして以下にまとめておく.

ILS

Step 1 初期解 $\boldsymbol{\sigma}$ を生成し, $\boldsymbol{\sigma}_{\rm seed} := \boldsymbol{\sigma}$, $\boldsymbol{\sigma}_{\rm best} := \boldsymbol{\sigma}$ とする.

Step 2 局所探索法により $\boldsymbol{\sigma}_{\rm seed}$ を改善し, $\boldsymbol{\sigma}$ とおく.

Step 3 $\boldsymbol{\sigma}$ が $\boldsymbol{\sigma}_{\rm best}$ よりも良ければ, $\boldsymbol{\sigma}_{\rm best} := \boldsymbol{\sigma}$ とする.

Step 4 ある停止条件が満たされれば $\boldsymbol{\sigma}_{\rm best}$ を出力して終了. そうでなければ $\boldsymbol{\sigma}_{\rm best}$ に少しランダムな変形を加えた新たな初期解 $\boldsymbol{\sigma}_{\rm seed}$ を生成し, 2 に戻る.

2.7 高速化

局所探索法の中で近傍解を評価する度に, 最適スケジュール問題を解いていたのでは非常に時間がかかってしまう. そこで本研究では, 以下のような高速化を行う.

車両 k が時刻 t 以降に客 $\sigma_k(h)$ のサービスを行うとして, それ以降の客 $\sigma_k(h), \sigma_k(h+1), \ldots, \sigma_k(n_k+1)$ をすべてサービスするのにかかる移動時間と時間枠コストの総和の最小値を $b_h^k(t)$ と定義し, 後向きコスト最小関数と呼ぶ. $b_h^k(t)$ は前向きコスト最小関数と対称的に漸化式

$$\begin{aligned} b_{n_k+1}^k(t) &= \min_{t \le s} p_0(s), \quad -\infty < t < +\infty \\ b_h^k(t) &= \min_{t \le s} \left\{ p_h^k(s) + w_h^k(s) \right\} \\ & \qquad 1 \le h \le n_k, \ -\infty < t < +\infty \end{aligned}$$

によって計算できる. ただし,

$$w_h^k(s) = \min_{s \le t'} \{ b_{h+1}^k(t' + q_h^k(t')) + q_h^k(t') \}$$

である．これらを用いると, ルート σ_k の時間枠コストと移動時間の総和の最小値は $\min_t f_h^k(t) + q_h^k(t) + b_{h+1}^k(t + q_h^k(t))$ によって得られ, その計算時間は $O(\Delta_k)$ である．

このことを利用して, 現在の解 $\boldsymbol{\sigma}$ の各車両 k の各客 $\sigma_k(h)$ に対して, f_h^k と b_h^k を保持しておけば, たとえば 2-opt* 近傍で σ_k と $\sigma_{k'}$ のルートの後半のパスを入れ替えるときは, σ_k の前半のパスの最後の客 $\sigma_k(h)$ の f_h^k と $\sigma_{k'}$ の後半のパスの最初の客 $\sigma_{k'}(h')$ の $b_{h'}^{k'}$ から, そのルートの最適スケジュールでのコストを

$$\begin{aligned} \min_t f_h^k(t) \quad &+ \quad q_{\sigma_k(h),\sigma_{k'}(h')}(t) \\ &+ \quad b_{h'}^{k'}(t + q_{\sigma_k(h),\sigma_{k'}(h')}(t)) \end{aligned}$$

によって求めることができる．残りの 2 つの近傍についても, 近傍内の解を適当な順序で探索することにより同様の高速化が行える．

2.8 計算実験

提案手法の性能を評価するため, 文献 [3] で提案されているベンチマーク問題例を用いて計算実験を行った．これらの問題例では, スケジュール期間は「朝」「日中」「夕方」の 3 期間から成り, すべての枝 (i, j) について, 日中の移動速度は一定, 朝と夕方の移動速度は日中よりも遅くなるよう移動時間関数 q_{ij} が与えられている．なお, 計算実験はすべて Intel Pentium 4 (2.8 GHz), 1 GB メモリを搭載したパーソナルコンピュータ上で行った．

移動時間の時刻依存性が小さい問題例および大きい問題例の 2 種類に対して, それぞれ 56 題ずつを解いた結果を表 2.1 に示す．また, 比較のため, すべての問題例に対して, 移動時間を平均値 (定数) で置き換えた問題例に対しても計算実験を行った．(ただし, 最終的な解の評価は時刻依存性を考慮して行った.) 各行は問題例のタイプを表し, p_{sum}, q_{sum} の各列は, 対応するタイプの問題例すべてに対する p_{sum}, q_{sum} の平均値をそれぞれ表す (a_{sum} の値は, すべての場合において 0 であったため省略).

表 2.1 より, p_{sum}, q_{sum} ともに「時刻依存」の方が「定数」よりも小さいことが確認でき, この差は, 移動時間の時刻依存性が大きい程顕著になっており, 時刻依存性を考慮した効果が表れている．

2.9 まとめ

本研究では, 従来の配送計画問題では定数として扱われていた移動時間を移動開始時刻の関数として, 時間依存配送計画問題の定式化を行った．そして, 与えられたルートの最適スケジュールを決定する動的計画法のアルゴリズムを部分アルゴリズムに用いて局所探索法に基づく 1 つのメタ解法を提案した．計算実験の結果では, 従来より柔軟性の高い配送計画が得られることが観測され, 本定式化の有効性が確認できた．

参考文献

[1] M. R. Garey and D. S. Johnson, *Computers and Intractability,* Freeman (1979).

[2] T. Ibaraki, S. Imahori, M. Kubo, T. Masuda, T. Uno and M. Yagiura, "Effective Local Search Algorithms for Routing and Scheduling Problems with General Time Window Constraints," *Transportation Science*, to appear.

[3] S. Ichoua, M. Gendreau, and J.Y. Potvin, Vehicle dispatching with time-dependent travel times, *European Journal of Operational Research*, vol. 144, pp. 379–396, 2003.

[4] M. M. Solomon, "The Vehicle Routing and Scheduling Problems with Time Window Constraints," *Operations Research*, Vol. 35, No. 2, pp. 254–265 (1987).

3 現実ネットワークのモデリング

インターネット, Web グラフをはじめ, 経済, マーケティング, 流行現象, 伝染病の伝播, 生態系, 人間関係など, 多くの領域で「ネットワーク」が見られる．近年のコンピュータ技術の発達によるデータ収集・解析能力の向上によって, このような現実のネットワークの性質が詳細に分析できるようになってきた．その結果, 現実のネットワークはまったくランダムなネットワークとは異なり, 特徴的な性質を持つということが分かってきた．

表 2.1: 時刻依存配送計画問題に対する計算結果

	時刻依存性 小				時刻依存性 大			
	時刻依存		定数		時刻依存		定数	
	p_{sum}	q_{sum}	p_{sum}	q_{sum}	p_{sum}	q_{sum}	p_{sum}	q_{sum}
C1	20.35	855.27	35.47	984.26	90.80	885.66	183.30	1301.37
C2	2.31	669.94	0.00	712.52	7.43	763.61	54.25	919.15
R1	32.47	1061.93	50.60	1188.67	43.41	921.41	94.92	1260.24
R2	5.04	904.40	19.62	1021.33	3.00	809.01	77.37	1139.08
RC1	50.10	1103.62	59.50	1298.58	55.23	967.13	96.89	1295.63
RC2	19.69	976.53	25.09	1140.38	12.40	877.58	106.79	1263.43

このようなネットワークの特性を調べることにより，様々な応用に際してアルゴリズムを適用する範囲を限定でき計算量の削減につなげられる可能性がある．そこで，本研究では，主に現実のネットワークの特性を反映する適切な数理モデルの構築と解析に重点を置き，その結果として，現実のネットワークにおいて，メタヒューリスティックスをはじめ，様々なアルゴリズムの計算量を削減することを目指している．

現実のネットワークは様々な性質を持つが，まず第一に，多くのネットワークがスケールフリーという性質を持つことが知られている．これは，次数分布がべき則に従う，つまり，次数（v に接続する辺数）k の点数の割合 $p(k)$ が $k^{-\gamma}$ に比例するというものである．インターネットのネットワーク構造や，WWW のハイパーリンク構造, human sexual network，遺伝子ネットワーク，食物連鎖，E-mail ネットワークなど，多くのネットワークがスケールフリーであることが知られている．

現実の複雑ネットワークは，スケールフリー性以外にも，例えばクラスタ係数に関しても特徴的な性質を持つ．各点 v のクラスタ係数は，v の次数を k_v とした時，その点の隣接点間の辺数を $k_v(k_v-1)/2$（つまり隣接点間辺数の取りうる最大値）で割ったものとして定義される．同じ次数 k の点のクラスタ係数の平均を $C(k)$，グラフ全体のクラスタ係数の平均を C と表記する．この時，多くの現実の複雑ネットワークは，$C(k) \propto k^{-\gamma'}$ $(\gamma' > 0)$ という性質を持ち，C はネットワークの規模に関わらず比較的大きい値を取るという性質を持つことが示されている．

また，隣接点の平均次数に関しても，k に関してべき則に従うという性質を持つことが多い．

平均点間距離に関しては，現実のネットワークでは，点数 n に対して $O(\log n)$ や $O(\log\log n)$ という観測がなされている．このように点数に比べて平均点間距離が小さい性質はスモールワールドと言われる．

これらの性質を持つモデルがこれまで様々なモデルが提案されてきた．複雑ネットワークを，ある種のランダムグラフと捉えたモデルも多々提案されている．それらの多くは，時間の経過とともに点も付け加えられていく「成長」(growth) と，新しく加わった点は次数の高い既存の点と高い確率で辺で繋がれる「優先的選択」(preferential attachment) という 2 つの原理を基本としている．その代表的な Barabási と Albert によるモデル（BA モデルと呼ぶ）は，詳しく解析され，$p(k) \propto k^{-3}$ であること，直径は $O(\log n/\log\log n)$ であることなどが証明されている．

BA モデルやそのバリエーションをはじめ,「成長」と「優先的選択」に基づくモデルによって良く説明できる現実のネットワークも多々存在する．しかし，すべてのネットワークがこのような原理に基づいてできているわけではない．例えば，会社や学校などの集団内の人間関係ネットワークの形成過程や，取引ネットワーク，サイト間相互リンクネットワークなど，点の増加や減少がネットワークの内部構造変化に対して十分遅いと考えられるものや，次数の高いものほど有利になることはないものにおいては，他の原理に基づいていると考える方が自然である．

このような,「成長」や「優先的選択」に基づかないネットワークの生成モデルとして，各点には重み（適応度）が確率的に与えられており，点 v_i と v_j の間には，v_i と v_j の重みの和や積（一般的には 2 点の重みの関数）に基づいて確率的に辺が張られるという原理で生成されるものがある．点

の重みが従う確率分布が指数分布やべき分布に従う場合，生成されるグラフはスケールフリーとなることが分かっている．この一般的なモデルのうち，特に，v_i と v_j の重みの和や積がある閾値を越える時，またその時に限るという原理で生成される閾値モデルというものがある．なお，辺の有無は確率的ではなく決定的に決まると制限しても本質的には変わらず現実性を失わない．

本年度は，この閾値モデルを提案し，重みが指数分布，パレート分布，ガウス分布，幾何分布に従う場合，生成されるグラフがスケールフリーとなること，生成されるグラフのクラスタ係数，隣接点平均次数は，次数に関してべき的に減少することを示した．これらは，現実のネットワークのものとも整合性を持つことを示している．さらに，この重み分布が生成されるメカニズムを調べ，重みが「優先的選択」に従って増加する自然なモデルにおいて重み分布が幾何分布に確率収束することを数学的に厳密に証明した．これらの結果は，閾値モデルは広い領域で現実のネットワークの形成メカニズムを説明できることを示している．

また，現実のネットワークに関する問題とアルゴリズムの研究として，通信ネットワークにおける高信頼度ネットワーク設計問題を扱い，そのアルゴリズム及び計算量を解析した．この設計問題を節点領域辺連結度（NA 辺連結度）増加問題として定式化し，2-NA 辺連結化問題は多項式時間で解けること，2-NA 辺連結化問題は NP 完全であることを証明した．

3.1 閾値モデル

n 点からなる点集合 $V = \{v_1, v_2, \ldots, v_n\}$ において，各点 $v_i \in V$ には重み $w_i \in \mathbb{R}$ が，確率密度関数 $f(w)$ に従って独立に与えられているとする．$f(w)$ の累積分布関数を $F(w) = \int_{-\infty}^{w} f(w')dw'$ と表記することにする．閾値 θ が与えられた時，辺集合は，$E \stackrel{\text{def}}{\Longleftrightarrow} \{(v_i, v_j) \mid w_i + w_j \geq \theta, v_i, v_j \in V, v_i \neq v_j\}$ として定義される．

閾値モデルは，人間関係ネットワークなどのモデルとして有効だと考えられる．例えば点を人間と考え，点の重みをその人間の活動レベル（交友関係を築く能力）だと考えると，活動レベルの和（一般的にはそれらの関数で良い）がある閾値を越えると人間関係ができると解釈できる．他にも，重みをお金と考え，自分と相手の元手の合計がある値を越えれば事業が起こせたり共同開発を行うと判断すると考えれば，企業間ネットワークの形成を説明できるとも解釈できる．これらの例をはじめ,「成長」や「優先的選択」に基づかないネットワークの形成モデルとして，閾値モデルが適用できる領域は多々あると考えられる．

閾値モデルで生成される無向グラフは，グラフ理論において閾値グラフ (threshold graph) として知られているものである．閾値グラフの点集合は，クリークと独立点集合（互いに隣接しない点集合）に分割でき，後者の点は孤立点を除いてすべてクリークの点と隣接しているという性質があることが分かっている．従って，一般的な閾値グラフであっても，クリークがハブに対応し，他の点はハブに接続するという，現実のネットワークの性質との適合性の高い描像が成り立っている．

なお，閾値グラフの直径は 2 なので，閾値モデルで生成されるグラフの平均点間距離は 2 以下である．

この閾値グラフにおいて重み分布を決めると，対応して次数分布やクラスタ係数などの具体的な形が得られる．なお，閾値モデルで生成される無向グラフ $G = (V, E)$ は有限グラフなので次数分布は離散的であるが，以後の解析においては，$n \to \infty$ の極限における次数分布を近似として使うことにする．

まず，$f(w)$ 及びその累積分布関数 $F(w)$ を用いて，次数分布，クラスタ係数，隣接点平均次数の一般形を与えておく．

$$k = n \int_{\theta - w}^{\infty} f(w')dw' = n[1 - F(\theta - w)] \quad (0 \leq k \leq n) \tag{2.27}$$

なので，次数分布 $p(k)$ は

$$p(k) = f(w)\frac{dw}{dk} = \frac{f(\theta - F^{-1}(1 - k/n))}{nf(F^{-1}(1 - k/n))} \tag{2.28}$$

と書ける．

また，次数 k の点の平均クラスタ係数 $C(k)$ は

以下のように書ける．

$$\begin{aligned} C(k) &= \frac{1}{2}\frac{1}{k(k-1)/2}\Big\{\int_w^\infty kf(w')\,dw' \\ &\quad + \int_{\theta-w}^{w} n(1-F(\theta-w'))f(w')\,dw'\Big\} \\ &= \Big\{-1+2\frac{k}{n} \\ &\quad + \Big(1-\frac{k}{n}\Big)F\Big(\theta-F^{-1}\Big(1-\frac{k}{n}\Big)\Big) \\ &\quad - \int_t^k \Big(1-\frac{k'}{n}\Big)p(k')\,dk'\Big\}\Big/\Big(\frac{k}{n}\Big)^2 \quad (2.29) \\ &\quad (t = n(1-F(\theta-F^{-1}(1-k/n)))) \end{aligned}$$

なお，重みが $\theta/2$ 以下（もしくは次数が $n(1-F(\theta/2))$ 以下）の時は，$C(k)=1$ である．

グラフ全体のクラスタ係数 C は，$C = \int_0^\infty C(k)p(k)dk$ である．

隣接点間の次数の相関を見るために，次数 k の点 v の隣接点の次数の和を k_2 として，隣接点の平均次数 k_2/k を調べる．

$$\begin{aligned} k_2 &= \int_{\theta-w}^{\infty} nf(w')n\left[1-F\left(\theta-w'\right)\right]dw' \\ &= n^2\Big\{\frac{k}{n} - \\ &\quad \int_{n[1-F(\theta-F^{-1}(1-k/n))]}^{n}\left(1-\frac{k'}{n}\right)p(k')dk'\Big\} \end{aligned} \quad (2.30)$$

であるため，

$$\begin{aligned} \frac{k_2}{k} &= n\Big\{1- \\ &\quad \frac{1}{k}\int_{n[1-F(\theta-F^{-1}(1-\frac{k}{n}))]}^{n}(n-k')p(k')dk'\Big\} \end{aligned} \quad (2.31)$$

と書ける．

重みが指数分布やパレート分布に従う場合は，次に述べるように，上で得られた関係式から解析的に次数分布，クラスタ係数，隣接点平均次数が求められる．

重みが指数分布 $f(w)=\lambda e^{-\lambda w}$ $(0\le w)$ に従う時は，

$$p(k) = \frac{ne^{-\lambda\theta}}{k^2} \quad (ne^{-\lambda\theta} \le k \le n) \qquad (2.32)$$

であり，$\gamma=2$ のべき則に従う．クラスタ係数については，

$$C(k) = \begin{cases} 1 \\ \quad (ne^{-\lambda\theta} \le k \le ne^{-\lambda\theta/2}) \\ \frac{n^2}{k^2}e^{-\lambda\theta}\left(1+\lambda\theta+2\ln\frac{k}{n}\right) \\ \quad (ne^{-\lambda\theta/2} < k \le n) \end{cases} \qquad (2.33)$$

となる．

式 (2.33) から，$C(k)\propto k^{-2}$ が分かる．この結果は，既存モデルや実データの解析から，$C(k)\propto k^{-\gamma'}$ $(\gamma'>0)$ であることが示されていることと整合性はあるが，代謝ネットワーク，インターネットや俳優の共演関係などの現実のネットワークの観測結果やなどのモデルでは，$C(k)\propto k^{-1}$ となっており，これらの例と比較する限り，重みが指数分布に従う閾値モデルは，べき指数に関してはやや外れがある．

グラフ全体のクラスタ係数は，

$$\begin{aligned} C &= \int_{ne^{-\lambda\theta}}^{n} C(k)p(k)dk \\ &= 1-\frac{4}{9}e^{-\lambda\theta/2}-\frac{5+3\lambda\theta}{9}e^{-2\lambda\theta} \end{aligned} \quad (2.34)$$

となる．

現実のネットワークでは，平均次数 $\langle k\rangle$ は，n とは独立に有限の値をとることことが分かっているが，本モデルでは，

$$\langle k\rangle = e^{-\lambda\theta}\left(n+\lambda\theta\right), \qquad (2.35)$$

となるため，$\theta\cong\lambda^{-1}\ln n$ となるように閾値 θ を設定することによって，n の大きさに関わらず $\langle k\rangle$ が有限の値に抑えられる．なお，この閾値の設定により，グラフ全体のクラスタ係数 C は $n\to\infty$ の極限でも 0 にならない．これも現実のネットワークの結果と整合性がある．

隣接点平均次数については，

$$\frac{k_2}{k} = \frac{n^2\mathrm{e}^{-\lambda\theta}}{k}\left(1+\lambda\theta+\ln\frac{k}{n}\right) \qquad (2.36)$$

となり，k に関して減少している．これから高い次数の点は低次数の点と結合しやすい傾向があることが分かる．現実のある種類のネットワークもこのような性質があることが分かっており，このことも現実のネットワークの結果と整合性があることを示している．

次に，パレート分布 $f(w) = \frac{a}{w_0}(\frac{w_0}{w})^{a+1}$ $(w \geq w_0 > 0, a > 0)$ に従う場合の結果を紹介する．パレート分布は，企業規模の分布などでも見られる．

この場合，次数分布は，

$$p(k) = \frac{n^{1/a}}{\left(\frac{\theta}{w_0}k^{1/a} - n^{1/a}\right)^{a+1}}. \quad (2.37)$$

となるため，

$n(w_0/\theta)^a \ll k < n$ であるとき，次のように近似できる．

$$p(k) \cong \left(\frac{w_0}{\theta}\right)^{a+1} n^{1/a} k^{-(a+1)/a} \quad (2.38)$$

これから，重み分布のパラメータ a によって，1 以上の任意の γ を実現することができる．

クラスタ係数についても，

$$\begin{aligned} C(k) &= \frac{n}{k}\left(\frac{w_0}{\theta - w_0\left(\frac{n}{k}\right)^{1/a}}\right)^a \\ &\quad + \frac{n^2 a}{k^2}\left(\frac{w_0}{\theta}\right)^{2a} \\ &\quad \times \int_{(n/k)^{1/a}(w_0/\theta)}^{1-(n/k)^{1/a}(w_0/\theta)} y^{-a}(1-y)^{-a-1}dy \\ &\quad \left(k > n\left(\frac{2w_0}{\theta}\right)^a\right) \end{aligned} \quad (2.39)$$

$$C(k) = 1 \quad \left(n\left(\frac{w_0}{\theta - w_0}\right)^a \leq k \leq n\left(\frac{2w_0}{\theta}\right)^a\right) \quad (2.40)$$

が得られる．これから，k が十分大きいところでは，$C(k) \propto k^{-1}$ と言える．これは現実のネットワークの観測結果と整合性がある．

隣接点平均次数も，

$$\begin{aligned} \frac{k_2}{k} &= \frac{n^2}{k}\left(\frac{w_0}{\theta - w_0}\right)^a \\ &\quad + \frac{n^2 a}{k}\left(\frac{w_0}{\theta}\right) \\ &\quad \times \int_{w_0/\theta}^{1-(n/k)^{1/a}(w_0/\theta)} y^{-a}(1-y)^{-a-1}dy \end{aligned} \quad (2.41)$$

として得られる．式 (2.41) から，k が十分大きいところでは，$k_2/k \propto k^{-1}$ と言える．このことから，指数分布の場合と同様に，高い次数の点は低次数の点と結合しやすい傾向があることが分かる．

なお，式 (2.39) と式 (2.41) から，$C(k)$ と k_2/k のべき指数は，γ にも a にも依存していないことが分かる．

重みがガウス分布や幾何分布に従う場合は，解析的に陽に次数分布，クラスタ係数，隣接点平均次数が求めることができないので，数値実験を行った．その結果，$p(k) \propto k^{-2}$，$C(k) \propto k^{-2}$，$k_2/k \propto k^{-1}$ であることが分かった．

3.2 高信頼度ネットワーク設計問題

グラフにおける点と点部分集合（領域）との間の連結度を表す概念として，節点領域連結（以下 NA 連結）というものが提案されている．NA 連結性は，通信ネットワークにおける様々な問題に適用できる概念である．サーバ配置問題では，同一コンテンツを提供する複数のサーバが存在する時（例えば WWW におけるミラーサーバ），クライアントはそれらのサーバのいずれか一つにアクセスできれば十分であるが，経路負荷分散の観点から，サーバ群に対して複数の独立な経路を確保できる方が望ましい．この時，サーバ群を一つの領域と考えれば，NA 連結性の問題として扱うことができる．また，通信ネットワークにおけるルーチング制御や設計にも適用できる．複数の外部ネットワークと複数の接続ポイントで接続しているネットワークにおいて，外部のホストと通信するためには，少なくともいずれか一つの接続ポイントへの可到達性が確保されている必要があるが，そのためには経路の負荷分散や耐故障性の観点から，少なくともいずれか一つの接続ポイントへの経路が複数独立に確保できていなければならない．この場合も，接続ポイントの集合を一つの領域と考えることで，NA 連結性の問題として扱うことができる．実際，接続ポイントを増やしたりリンクを追加することで，独立な経路数を確保することや，ドメイン内ルーチングにおいて，冗長なリンクを落として縮約したネットワークをデータとして保持することで（例えば OSPF のようなプロトコルにおいて），ルーチングテーブルの記憶に必要なデータ量を圧縮することができる．

NA 連結性については様々な性質が明らかにされている．例えば，領域に含まれる節点を最小限の個数だけ増やすことによって所望の NA（辺，

点）連結度に上げることが多項式時間で可能なこと，NA 連結度や節点領域間距離を保存する枝数最小の全域部分グラフを求める問題は NP 困難であるが，疎な全域部分グラフならば多項式時間で得られることなどが分かっている．

このような問題に対して，最小数の辺を付加して所望の NA 連結度に増加する問題が考えられる．これは，上記の通信ネットワークの例においては，外部ネットワークへの接続ポイントへの独立な経路数を増やすために，最小コストでリンクを増設する設計問題に対応する．

本研究では，最小辺付加 NA 枝連結度増加問題を扱った．その結果，0-NA 辺連結領域グラフを最小辺数の付加で 1-NA 辺連結領域グラフにする問題は NP 完全であることを証明した．さらに，1-NA 辺連結領域グラフおよび 0-NA 辺連結領域グラフを最小辺数の付加で 2-NA 辺連結領域グラフにすることは多項式時間で可能であることを示した．

3.3 まとめ

本年度は，閾値モデルにおいて，重みが指数分布，パレート分布，ガウス分布，幾何分布に従う場合，生成されるグラフがスケールフリーとなること，生成されるグラフのクラスタ係数，隣接点平均次数は，次数に関してべき的に減少することを示した．これらは，現実のネットワークのものとも整合性を持つことを示している．さらに，この重み分布が生成されるメカニズムを調べ，重みが「優先的選択」に従って増加する自然なモデルにおいて重み分布が幾何分布に確率収束することを数学的に厳密に証明した．これらの結果は，閾値モデルは広い領域で現実のネットワークの形成メカニズムを説明できることを示している．

また，現実のネットワークに関する問題とアルゴリズムの研究として，通信ネットワークにおける高信頼度ネットワーク設計問題を扱い，そのアルゴリズム及び計算量を解析した．この設計問題を節点領域辺連結度（NA 辺連結度）増加問題として定式化し，2-NA 辺連結化問題は多項式時間で解けること，1-NA 辺連結化問題は NP 完全であることを証明した．

4 マトロイド構造と貪欲アルゴリズム

いわゆるマトロイド構造を有する組合せ最適化問題に対して貪欲アルゴリズムが最適解を見出すが、マトロイド構造をもたない問題に対してもしばしば貪欲アルゴリズムが効率よく近似最適解を見出す。そのような観点から、近似あるいはヒューリスティックアルゴリズムにおける貪欲アルゴリズムの重要性が認識されている。本研究は、貪欲アルゴリズムの本質を解明し、より広い枠組みで有効な貪欲アルゴリズムの設計を可能にする基礎理論の構築を目的にし、研究を進めている。

研究業績一覧

著書

1. T. Ibaraki, K. Nonobe and M. Yagiura, eds.: “Metaheuristics—Progress as Real Problem Solvers”, Springer, （刊行予定）.
   概要: The framework of metaheuristics can produce robust and efficient algorithms for many computationally hard problems in real-world applications. This book comprises the papers carefully selected from those presented at the Fifth Metaheuristics International Conference (MIC2003). The book features those papers describing applications of metaheuristics as real problem solving tools, and also contains those discussing methodologies of metaheuristics.

2. 柳浦 睦憲 (分担執筆):
   “簡単そうで難しい組合せ最適化 — 身近な話題から”, 数理工学のすすめ（改訂版）, 現代数学社, 2005.
   概要: 計算困難な組合せ最適化問題に対するさまざまな現実的アプローチを身近な例を題材に取って解説する．具体的には，分枝限定法，動的計画法，欲張り法，局所探索法，メタ戦略などを概観したのち，近似解法の理論的成果に関しても触れる．

学術論文

1. S. Fujishige:
"Dual Greedy Polyhedra, Choice Functions, and Abstract Convex Geometries", Discrete Optimization, 1, 41–49, 2004.
概要: We consider a system of linear inequalities and its associated polyhedron for which we can maximize any linear objective function by finding tight inequalities at an optimal solution in a greedy way. We call such a system of inequalities a dual greedy system and its associated polyhedron a dual greedy polyhedron. Such dual greedy systems have been considered by Faigle and Kern, and Krüger for antichains of partially ordered sets, and by Kashiwabara and Okamoto for extreme points of abstract convex geometries. Faigle and Kern also considered dual greedy systems in a more general framework than antichains. A related dual greedy algorithm was proposed by Frank for a class of lattice polyhedra. In the present paper we show relationships among dual greedy systems, substitutable choice functions, and abstract convex geometries. We also examine the submodularity and facial structures of the dual greedy polyhedra determined by dual greedy systems. Furthermore, we consider an extension of the class of dual greedy polyhedra.

2. T. Ibaraki, S. Imahori, M. Kubo, T. Masuda, T. Uno and M. Yagiura:
"Effective Local Search Algorithms for Routing and Scheduling Problems with General Time-Window Constraints", Transportation Science, (掲載予定).
概要: We propose local search algorithms for the vehicle routing problem with soft time window constraints. The time window constraint for each customer is treated as a penalty function, which is very general in the sense that it can be non-convex and discontinuous as long as it is piecewise linear. In our algorithm, we use local search to assign customers to vehicles and to find orders of customers for vehicles to visit. It employs an advanced neighborhood, called the cyclic exchange neighborhood, in addition to standard neighborhoods for the vehicle routing problem. After fixing the order of customers for a vehicle to visit, we must determine the optimal start times of processing at customers so that the total penalty is minimized. We show that this problem can be efficiently solved by using dynamic programming, which is then incorporated in our algorithm. We then report computational results for various benchmark instances of the vehicle routing problem. The generality of time window constraints allows us to handle a wide variety of scheduling problems. As such an example, we mention in this paper an application to a production scheduling problem with inventory cost, and report computational results for real world instances.

3. T. Ibaraki, Y. Vaxès, X-G. Yang:
"Lowering eccentricity of a tree by node-upgrading", Networks, (掲載予定).
概要: The eccentricity lowering problem is to reduce the eccentricity of a network by upgrading some nodes (i.e., shrinking the lengths of the edges incident to such nodes). We consider two types of node-upgrading strategies, i.e., a continuous upgrading strategy and a discrete upgrading strategy, where the improvement under the first strategy is a continuous variable, and the improvement under the second strategy is a fixed amount. These problems are hard even to approximate, for general graphs. Therefore we restrict our attention to graphs with simple structures. Assuming that the graph $G = (V, E)$ is a tree, we show that the eccentricity lowering problem under the continuous node-upgrading strat-

egy can be reduced to the eccentricity lowering problem under the continuous edge-upgrading strategy, and can be solved by an $O(|V|\log|V|)$ time algorithm. We also show that the problem for a tree is NP-hard under the discrete upgrading strategy, but admits a fully polynomial approximation scheme, if the graph is a line.

4. S. Imahori, M. Yagiura and T. Ibaraki:
"Improved Local Search Algorithms for the Rectangle Packing Problem with General Spatial Costs", European Journal of Operational Research, 167, 48-67, 2005.
概要: The rectangle packing problem with general spatial costs is to pack given rectangles without overlap in the plane so that the maximum cost of the rectangles is minimized. This problem is very general, and various types of packing problems and scheduling problems can be formulated in this form. For this problem, we have previously presented local search algorithms using a pair of permutations of rectangles to represent a solution. In this paper, we propose speed-up techniques to evaluate solutions in various neighborhoods. Computational results for the rectangle packing problem and a real-world scheduling problem exhibit good prospects of the proposed techniques.

5. S. Imahori, M. Yagiura, S. Umetani, S. Adachi and T. Ibaraki:
"Local Search Algorithms for the Two Dimensional Cutting Stock Problem with a Given Number of Patterns", T. Ibaraki, K. Nonobe and M. Yagiura, eds., Metaheuristics—Progress as Real Problem Solvers, Springer, (掲載予定).
概要: We consider the two-dimensional cutting stock problem that arises in many applications in industries. In recent industrial applications, it is argued that the setup cost for changing patterns becomes more dominant and it is impractical to use many different cutting patterns. Therefore, we consider the pattern restricted two-dimensional cutting stock problem, in which the total number of applications of cutting patterns is minimized while the number of different cutting patterns is given as a parameter n. For this problem, we develop local search algorithms. As the neighborhood size plays a crucial role in determining the efficiency of local search, we propose to use linear programming techniques for the purpose of restricting the number of solutions in the neighborhood. In this process, to generate a cutting pattern, it is required to place all the given products (rectangles) into the stock sheet (two-dimensional area) without mutual overlap. For this purpose, we develop a heuristic algorithm using an existing rectangle packing algorithm with the sequence pair coding scheme. Finally, we generate random test instances of this problem and conduct computational experiments, to evaluate the effectiveness of the proposed algorithms.

6. N. Masuda, H. Miwa, N. Konno:
"Analysis of scale-free networks based on threshold graph with intrinsic vertex weights", Physical Review E, Vol. 70, No. 3, 036124, 2004年11月.
概要: 現実のネットワークの生成モデルとして，閾値モデルを提案し，重みが指数分布，パレート分布に従う場合，生成されるグラフがスケールフリーとなること，生成されるグラフのクラスタ係数，隣接点平均次数は，次数に関してべき的に減少することを示した.

7. H. Miwa, H. Ito:
"NA-Edge-Connectivity Augmentation Problems by Adding Edges", Journal of the Operations Research Society of Japan, Vol. 47, No. 4, pp. 224-243, 2004年12月.
概要: 現実のネットワークに関する問題とア

ルゴリズムの研究として，通信ネットワークにおける高信頼度ネットワーク設計問題を扱い，そのアルゴリズム及び計算量を解析した．この設計問題を節点領域辺連結度（NA 辺連結度）増加問題として定式化し，2-NA 辺連結化問題は多項式時間で解けること，2-NA 辺連結化問題は NP 完全であることを証明した．

8. H. Ono, M. Yagiura and T. Ibaraki:
"A Decomposability Index in Logical Analysis of Data", Discrete Applied Mathematics, 142, 165-180, 2004.
概要: Logical analysis of data (LAD) is one of the methodologies for extracting knowledge in the form of a Boolean function f from a given pair of data sets (T, F) on attributes set S of size n, in which T (resp., F) $\subseteq \{0,1\}^n$ denotes a set of positive (resp., negative) examples for the phenomenon under consideration. In this paper, we consider the case in which extracted knowledge f has a decomposable structure; $f(x) = g(x[S_0], h(x[S_1]))$ for some $S_0, S_1 \subseteq S$ and Boolean functions g and h, where $x[I]$ denotes the projection of vector x on I. In order to detect meaningful decomposable structures, however, it is considered that the sizes $|T|$ and $|F|$ must be sufficiently large. In this paper, based on probabilistic analysis, we provide an index for such indispensable number of examples to detect decomposability; we claim that there exist many deceptive decomposable structures of (T, F) if $|T||F| \leq 2^{n-1}$. The computational results on synthetically generated data sets and real-world data sets show that the above index gives a good lower bound on the indispensable data size.

9. M. Yagiura, T. Ibaraki and F. Glover:
"An Ejection Chain Approach for the Generalized Assignment Problem", INFORMS Journal on Computing, 16, 133-151, 2004.
概要: We propose a tabu search algorithm for the generalized assignment problem, which is one of the representative combinatorial optimization problems known to be NP-hard. The algorithm features an ejection chain approach, which is embedded in a neighborhood construction to create more complex and powerful moves. We also incorporate an adaptive mechanism for adjusting search parameters, to maintain a balance between visits to feasible and infeasible regions. Computational results on benchmark instances of small sizes show that the method obtains solutions that are optimal or that deviate by at most 0.16% from the best known solutions. Comparisons with other approaches from the literature show that, for instances of larger sizes, our method obtains the best solutions among all heuristics tested.

10. M. Yagiura, T. Ibaraki and F. Glover:
"A Path Relinking Approach with Ejection Chains for the Generalized Assignment Problem", European Journal of Operational Research, （掲載予定）.
概要: The generalized assignment problem is a classical combinatorial optimization problem known to be NP-hard. It can model a variety of real world applications in location, allocation, machine assignment, and supply chains. The problem has been studied since the late 1960s, and computer codes for practical applications emerged in the early 1970s. We propose a new algorithm for this problem that proves to be more effective than previously existing methods. The algorithm features a path relinking approach, which is a mechanism for generating new solutions by combining two or more reference solutions. It also features an ejection chain approach, which is embedded in a neighborhood construction to create more complex and powerful moves. Computational comparisons on benchmark instances show that the method is not only

effective in general, but is especially effective for types D and E instances, which are known to be very difficult.

11. M. Yagiura, S. Iwasaki, T. Ibaraki and F. Glover:
"A Very Large-Scale Neighborhood Search Algorithm for the Multi-Resource Generalized Assignment Problem", Discrete Optimization, 1, 87-98, 2004.
概要: We propose a metaheuristic algorithm for the multi-resource generalized assignment problem (MRGAP). MRGAP is a generalization of the generalized assignment problem, which is one of the representative combinatorial optimization problems known to be NP-hard. The algorithm features a very large-scale neighborhood search, which is a mechanism of conducting the search with complex and powerful moves, where the resulting neighborhood is efficiently searched via the improvement graph. We also incorporate an adaptive mechanism for adjusting search parameters, to maintain a balance between visits to feasible and infeasible regions. Computational comparisons on benchmark instances show that the method is effective, especially for type D and E instances, which are known to be quite difficult.

12. M. Yagiura, M. Kishida and T. Ibaraki:
"A 3-Flip Neighborhood Local Search for the Set Covering Problem", European Journal of Operational Research, (掲載予定).
概要: The set covering problem (SCP) calls for a minimum cost family of subsets from n given subsets, which together covers the entire ground set. In this paper, we propose a local search algorithm for SCP, which has the following three characteristics. (1) The use of 3-flip neighborhood, which is the set of solutions obtainable from the current solution by exchanging at most three subsets. As the size of 3-flip neighborhood is $O(n^3)$, the neighborhood search becomes expensive if implemented naively. To overcome this, we propose an efficient implementation that reduces the number of candidates in the neighborhood without sacrificing the solution quality. (2) We allow the search to visit the infeasible region, and incorporate the strategic oscillation technique realized by adaptive control of penalty weights. (3) The size reduction of the problem by using the information from the Lagrangian relaxation is incorporated, which is indispensable for solving very large instances. According to computational comparisons on benchmark instances with other existing heuristic algorithms for SCP, our algorithm performs quite effectively for various types of problems, especially for very large-scale instances.

研究会等

1. 原田大輔，千代延大造，巳波弘佳:
"A Probablistic Analysis of a Netwok Model based on a generalization of the Polya's Urn Problem", ネットワーク生態学 2005 シンポジウム, 2005 年 3 月.
概要: 現実のネットワークの生成モデルである閾値モデルにおいて，この重み分布が生成されるメカニズムを調べ，重みが「優先的選択」に従って増加する自然なモデルにおいて，重み分布が幾何分布に確率収束することを数学的に厳密に証明した．さらに，重みが幾何分布に従う場合，生成されるグラフがスケールフリーとなることを示した.

2. H. Hashimoto, T. Ibaraki, S. Imahori and M. Yagiura:
"A Local Search Algorithm for Routing and Scheduling Problems with Time Window and Traveling Time Constraints", Proceedings of the International Symposium on Scheduling (ISS2004), 143-146, 2004.
概要: We generalize the standard vehicle routing problem by allowing soft time

window and soft traveling time constraints, and propose a local search algorithm, where both constraints are treated as cost functions. With the proposed generalization, the problem becomes very general, and can treat various scheduling problems, e.g., with earliness and tardiness costs, and flexible processing time. In our algorithm, local search is used to determine routes. After fixing the route for a vehicle, we must determine the optimal start times of processing at customers so that the total cost is minimized. This subproblem is NP-hard when cost functions are general, and can be efficiently solved with dynamic programming when traveling cost functions are convex. We then report computational results for benchmark instances, and confirm the usefulness of the proposed generalization.

3. 巳波弘佳，増田直紀，今野紀雄:
“スケールフリー性を持つ閾値モデルの解析”, ネットワーク生態学2005シンポジウム, 2005年3月.
概要: 現実のネットワークの生成モデルである閾値モデルにおいて，重みがガウス分布に従う場合，生成されるグラフがスケールフリーとなること，生成されるグラフのクラスタ係数，隣接点平均次数は，次数に関してべき的に減少することを示した.

4. S. Umetani, M. Yagiura, T. Ibaraki:
“One-dimensional cutting stock problem with a given number of setups: a hybrid approach of metaheuristics and linear programming”, Proceedings of the 1st International Workshop on Hybrid Metaheuristics (HM2004), 101-114, 2004.
概要: One-dimensional cutting stock problem (1D-CSP) is one of the representative combinatorial optimization problems, and arises in many industries. Since the setup costs for switching different cutting patterns become more dominant in recent cutting industry, we consider a variant of 1D-CSP, called the pattern restricted problem (PRP), which minimizes the number of stock rolls while the number of different cutting patterns is constrained within a bound given by users. For this problem, we proposed a local search algorithm which alternately uses two types of local search processes with the 1-add and shift neighborhoods. To improve the performance of the local search algorithm, we incorporated it with linear programming (LP) techniques, which restrict the number of solutions in the neighborhoods and solve a large number of associated LP problems quickly. Through computational experiments, we observed that the new algorithm obtains solutions of better quality to other existing approaches.

学会大会等

1. T. Ibaraki, S. Imahori, K. Nonobe, K. Sobue, T. Uno and M. Yagiura:
“An Iterated Local Search Algorithm for the Vehicle Routing Problem with Convex Time Penalty Functions”, 35th Annual Conference of the Italian Operations Research Society (AIRO), 2004.

2. S. Imahori, M. Yagiura, S. Umetani, S. Adachi and T. Ibaraki:
“Local Search Algorithms for Two-Dimensional Cutting Stock Problem with a Given Number of Patterns”, The First ESICUP (EURO Special Interest Group on Cutting and Packing) Meeting, 2004.

3. K. Nonobe and T. Ibaraki:
“A Metaheuristic Algorithm for RCPSP with Multiple-Modes and Generalized Precedence Constraints”, CORS/SCRO-INFORMS International Meeting, 2004.

4. S. Umetani, M. Yagiura and T. Ibaraki:
“A Local Search Approach to the Pattern Restricted 1D-CSP”, The First ESICUP

(EURO Special Interest Group on Cutting and Packing) Meeting, 2004.

5. S. Umetani, M. Yagiura and T. Ibaraki: "A Variable Neighborhood Search for Cutting Stock Problem with Given Number of Patterns", CORS/SCRO-INFORMS International Meeting, 2004.

6. 柳浦睦憲: "時間枠つき配送計画問題に対する数理的アプローチ", 日本オペレーションズ・リサーチ学会 関西支部講演会 (招待講演), 2004.

7. M. Yagiura, T. Ibaraki and F. Glover: "A Path Relinking Approach with Ejection Chains for the Generalized Assignment Problem", CORS/SCRO-INFORMS International Meeting, 2004.

8. M. Yagiura and T. Ibaraki: "Recent Metaheuristic Algorithms for the Generalized Assignment Problem", Proceedings of the International Conference on Informatics Research for Development of Knowledge Society Infrastructure (ICKS2004), 229-237, 2004.

9. 柳浦睦憲: "メタヒューリスティクスに基づく問題解決エンジン", 電子情報通信学会総合大会, 2005.

C11: 大量データ処理のための領域効率の良いアルゴリズム

定兼 邦彦　山下 雅史　小野 廣隆

九州大学 大学院 システム情報学研究院
〒 812-8581 福岡市東区箱崎 6-10-1
{sada,mak,ono}@csce.kyushu-u.ac.jp

1　はじめに

本研究では主に大量データ処理のための領域効率の良いアルゴリズムの開発を行っている．インターネットや情報処理技術の発達により，大量の電子化されたデータが存在し，それらの有効活用，例えば，大量データからの高速な検索や知識発見を行うことが重要となる．このときに問題となるのは，データ処理の時間計算量および領域計算量である．本研究では計算量について従来とは異なるモデルを用い，より現実的なアルゴリズムの開発と評価を行っている．

領域計算量については，現在広く用いられている計算モデルではメモリセルの数により計算量を定義しているが，これは現実のプロセッサの構成を反映していない．なぜなら，1 つのセルはアルゴリズムで用いるポインタなどを格納するため，必要なセルのサイズは扱うデータ数に依存するが，従来モデルではこれを定数としているからである．具体的には，n 個のデータを扱うにはポインタのサイズは $\log_2 n$ ビット必要となり，大量のデータを扱う場合にはこのポインタのサイズを無視することができなくなる．本研究ではアルゴリズムの領域計算量はビット数で数える．これにより，従来のモデルより現実的な評価が可能となる．

時間計算量に関しても，現実のプロセッサの能力を考慮した評価を行う．通常は比較モデルやランダムアクセスモデル (RAM) が用いられるが，本研究ではワード RAM を用いる．このモデルでは $O(\log U)$ ビット (U はメモリサイズ) の数値演算やビット演算が定数時間で行える．ワード RAM ではビット演算を用いて一種の並列処理を行うことで時間計算量を落とすことができる．これは現実のプロセッサで可能であり，またこのようなビット数の制限がない RAM よりも現実的である．

本研究で扱うデータは Web ページなどのテキスト文書や，Web ページのリンク構造を表すグラフ等である．そして，文書の検索や，Web ページの検索，分類などを行う．文書の検索は，Web ページだけでなく，DNA 配列を表す文字列なども含む．これらのデータ量は膨大であるため，領域効率の良いアルゴリズムとデータ構造が必要である．例えば，人間の DNA 配列は約 30 億個の A, T, G, C の文字列として表される．1 つの文字は 2 ビットで表現できるため，文字列のサイズは約 750MB となる．一方，この文字列から検索を行うためのデータ構造である接尾辞配列は，ポインタが 32 ビットであるためサイズが約 12GB となってしまう．一般に，文字列長を n，アルファベットサイズを σ とすると，文字列サイズは $n \log \sigma$ ビット，データ構造のサイズは $O(n \log n)$ ビットとなる．このデータ構造のサイズを，検索速度を落とさずに $O(n \log \sigma)$ ビットにすることが目標である．さらに，オーダの評価のみではなく，定数項を小さくすることも目標である．究極的には，データ構造のサイズを文字列の圧縮率に対する情報理論的な下限と一致させることが目標である．また，文字列のみではなく，グラフ構造を表現するデータ構造のサイズの削減なども行う．

Web ページの検索では，データ量が非常に多いため，データ量の削減も必要である．また，検索結果を人間が見やすくするために，類似ページを 1 つにまとめたり，価値のあるページを抜き出すことが必要である．従来は Web ページ中の単語の頻度を用いる手法が用いられていたが，スパムページの存在により検索精度が下がっている．よって近年は Web のリンク構造を用いてページの価値を定義する手法が主流となっている．本研究ではこの手法の発展を目指している．

2 今年度の成果

2.1 Dynamic Dictionary Matching

Dynamic dictionary matching 問題とは，パタン集合 $\{P_1, P_2, \ldots, P_k\}$ とテキスト T に対し，T に現れるすべてのパタンの出現位置を求める問題であり，新しいDNA配列と既知の配列の一致を求めることに用いられる．この問題に対し，パタン集合を格納するデータ構造で，サイズが $O(d)$ ビット (d はパタンの長さの合計，アルファベットサイズは定数とする)，問い合わせが $O((|T|+occ)\log^2 d)$ 時間 (occ はパタンの出現回数)，パタン P の挿入削除が $O(|P|\log^2 d)$ 時間のデータ構造を開発した．

Dynamic dictionary matching 問題を解くために，まず動的更新の可能な圧縮接尾辞木のデータ構造を提案した．接尾辞木の巡回，接尾辞リンクの計算が $O(\log d)$ 時間，文字列ラベルの復元が $O(\log^2 d)$ 時間でてき，パタン P の挿入削除が $O(|P|\log^2 d)$ 時間でできる．また，木を表現するバランス括弧列表現の更新を $O(\log n/\log\log n)$ 時間で行うアルゴリズムも提案した．これらを用いることで，Dynamic dictonionary matching 問題を解くことができる．

2.2 Web サイト検索のためのランキング手法

Web サイトを検索する場合，非常に多くのページから価値のあるページを抜き出すことが必要になる．Google で用いられている PageRank 法は，Web ページのリンク構造を用いたページのランキング法で，成功を収めている．しかし，この手法を 1 つの Web サイト内のランキングに用いると不都合が生じる．なぜなら，PageRank ではトップページに高いランクが与えられるが，そこはインデックスページであり細かい情報を持たないからである．よって，サイト内検索に対しては異なるランキング手法が必要となる．

本研究ではホットリンクと呼ばれるリンクを用いてランキングを行う．これは Web ページの作者が特定のコンテンツへ直接ジャンプするために設定したリンクのことである．このホットリンクを全体のリンク構造から自動的に推定し，ページのランク付けを行う．この手法により，サイト内の重要なコンテンツページに高いランクを割り当てることができるようになった．

2.3 二次記憶上の圧縮接尾辞配列

圧縮接尾辞配列は文字列検索のための省スペースなデータ構造であるが，データ構造のサイズを小さくするために要素の差分を用いて表現をしているため，メモリ参照の局所性がなかった．本研究ではこのデータ構造を改良し，二次記憶や，分散メモリ環境でも効率よく動作するようにした．

2.4 無線アドホックネットワークでのブロードキャスト問題

無線アドホックネットワークは，ネットワークの構造が頻繁に変化するため，さまざまな問題が生じる．本研究ではその中で，同一データを全ノードに送信するための電力消費の最小化問題を扱っている．ノード間の距離はあらかじめ分からないため，アルゴリズムの評価は競合比を用いる．つまり，距離が分かっている場合の最適アルゴリズムでの電力消費の何倍以内になるかという評価を用いる．この問題に対し，最悪の競合比が $3/2+\sqrt{2}$ となるオンラインアルゴリズムを提案した．また，このアルゴリズムは最適であることも示した．

2.5 進化系統樹の作成

生物の進化を表す系統樹の作成について以下の問題を扱った．いくつかの部分的な系統樹が与えられたとき，それらの部分木全てを含む系統樹で，部分木のサイズが最も大きくなるものを求める (Maximum agreement supertree problem, MASP)．この問題に対して，計算量の解析とアルゴリズムの開発を行った．入力の木の数が 2 の場合，または木の次数が 2 で入力の木の数が定数の場合は多項式時間で解けるが，木の数が 3 以上で木の次数に制限がない場合は NP 困難であることを示した．また近似アルゴリズムも示した．

研究業績一覧

学術論文

1. Kunihiko Sadakane, Nadia Takki-Chebihi, Takeshi Tokuyama:
"Combinatorics and algorithms for low-discrepancy roundings of a real sequence", Theoretical Computer Science, 331(1), 23–36, Feb. 2005.
概要: We discuss the problem of computing all the integer sequences obtained by rounding an input sequence of n real numbers such that the discrepancy between the input sequence and each output binary sequence is less than one. The problem arises in the design of digital halftoning methods in computer graphics. We show that the number of such roundings is at most n+1 if we consider the discrepancy with respect to the set of all subintervals, and give an efficient algorithm to report all of them. Then, we give an optimal method to construct a compact graph to represent the set of global roundings satisfying a weaker discrepancy condition.

2. J. Jansson, H.-K. Ng, K. Sadakane, W.-K. Sung:
"Rooted Maximum Agreement Supertrees", Algorithmica, (掲載予定).
概要: Given a set $\mathcal{T}$ of rooted, unordered trees, where each $T_i \in \mathcal{T}$ is distinctly leaf-labeled by a set $\Lambda(T_i)$ and where the sets $\Lambda(T_i)$ may overlap, the maximum agreement supertree problem (MASP) is to construct a distinctly leaf-labeled tree Q with leaf set $\Lambda(Q) \subseteq \bigcup_{T_i \in \mathcal{T}} \Lambda(T_i)$ such that $|\Lambda(Q)|$ is maximized and for each $T_i \in \mathcal{T}$, the topological restriction of T_i to $\Lambda(Q)$ is isomorphic to the topological restriction of Q to $\Lambda(T_i)$. Let $n = \left|\bigcup_{T_i \in \mathcal{T}} \Lambda(T_i)\right|$, $k = |\mathcal{T}|$, and $D = \max_{T_i \in \mathcal{T}} \{\deg(T_i)\}$. We first show that MASP with $k = 2$ can be solved in $O\left(\sqrt{D}\, n \log(2n/D)\right)$ time, which is $O(n \log n)$ when $D = O(1)$ and $O(n^{1.5})$ when D is unrestricted. We then present an algorithm for MASP with $D = 2$ whose running time is polynomial if $k = O(1)$. On the other hand, we prove that MASP is NP-hard for any fixed $k \geq 3$ when D is unrestricted, and also NP-hard for any fixed $D \geq 2$ when k is unrestricted even if each input tree is required to contain at most three leaves. Finally, we describe a polynomial-time $(n/\log n)$-approximation algorithm for MASP.

3. Y. Handa, H. Ono, K. Sadakane, M. Yamashita:
"Neighborhood Composition: A Parallelization of Local Search Algorithms", Recent Advances in Parallel Virtual Machine and Message Passing Interface, Proceedings, LNCS 3241, 155–163, Sep. 2004.
概要: To practically solve NP-hard combinatorial optimizationproblems, local search algorithms and their parallel implementations on PVM or MPI have been frequently discussed. Since a huge number of neighbors may be examined to discover a locally optimal neighbor in each of local search calls, many of parallelization schemes, excluding so-called the multi-start parallel scheme, try to extract parallelism from a local search by distributing the examinations of neighbors to processors. However, in straightforward implementations, when the next local search starts, all the processors will be assigned to the neighbors of the latest solution, and the results of all (but one) examinations in the previous local search are thus discarded in vain, despite that they would contain useful information on further search. This paper explores the possibility of extracting information even from unsuccessful neighbor examinations in a systematic way to boost parallel local search algorithms. Our key concept is neighborhood composition. We demon-

strate how this idea improves parallel implementations on PVM, by taking as examples well-known local search algorithms for the Traveling Salesman Problem.

4. Ho-Leung Chan, Wing-Kai Hon, Tak-Wah Lam, Kunihiko Sadakane:
"Dynamic Dictionary Matching and Compressed Suffix Trees", Proceedings of ACM-SIAM Symposium on Discrete Algorithms, PR118, 13–22, Jan. 2005.
概要: Let T be a string with n characters over an alphabet of constant size. The recent breakthrough on compressed indexing allows us to build an index for T in optimal space (i.e., $O(n)$ bits), while supporting very efficient pattern matching. Yet the compressed nature of such indexes also makes them difficult to update dynamically. This paper extends the work on optimal-space indexing to a dynamic collection of texts. Our first result is a compressed solution to the *library management* problem, where we show an index of $O(n)$ bits for a text collection $\mathcal{L}$ of total length n, which can be updated in $O(|T| \log n)$ time when a text T is inserted or deleted from $\mathcal{L}$; also, the index supports searching the occurrences of any pattern P in all texts in $\mathcal{L}$ in $O(|P| \log n + occ \log^2 n)$ time, where occ is the number of occurrences. Our second result is a compressed solution to the *dictionary matching* problem, where we show an index of $O(d)$ bits for a pattern collection $\mathcal{D}$ of total length d, which can be updated in $O(|P| \log^2 d)$ time when a pattern P is inserted or deleted from $\mathcal{D}$; also, the index supports searching the occurrences of all patterns of $\mathcal{D}$ in any text T in $O\big((|T| + occ) \log^2 d\big)$ time. When compared with the $O(d \log d)$-bit suffix tree based solution of Amir *et al.*, the compact solution increases the query time by roughly a factor of $\log d$ only. The solution of the dictionary matching problem is based on a new compressed representation of a suffix tree. Precisely, we give $O(n)$-bit representation of a suffix tree for a dynamic collection of texts whose total length is n, which supports insertion and deletion of a text T in $O(|T| \log^2 n)$ time, as well as all suffix tree traversal operations, including forward and backward suffix links. This work can be regarded as a generalization of the compressed representation of static texts. In the study of the above result, we also derive the first $O(n)$-bit representation for maintaining n pairs of balanced parentheses in $O(\log n / \log \log n)$ time per operation, matching the time complexity of the previous $O(n \log n)$-bit solution.

5. S. Kutten, H. Ono, D. Peleg, K. Sadakane, M. Yamashita:
"Energy-Optimal Online Algorithms for Broadcasting in Wireless Networks", Proceedings of Second Annual Conference on Wireless On-demand Network Systems and Services (WONS), 125–130, Jan. 2005.
概要: We consider problems related to the design of energy-efficient online message broadcasting protocols in ad-hoc wireless networks. Recent developments in portable wireless devices with limited power resources have led to considerable interest in problems involving the construction of energy-efficient multicast trees in the network. Wireless devices can control their transmission power in order to save power consumption whenever the distance to the intended destination of the transmission is known. The attenuation of a signal with power P_s is $P_r = \frac{P_s}{d(s,t)^\delta}$, where $d(s,t)$ is the distance between hosts s and t, and $\delta \geq 1$ is the *distance-power gradient*. A message can be successfully decoded if P_r is no less than a constant γ. Therefore the *transmission range* of a host s, namely, the maximum distance to which a message can be successfully delivered from s, is $(P_s/\gamma)^{1/\delta}$.

Power control also has a positive effect on reducing the number of transmission collisions between nearby senders. The problem studied here concerns a single sender which has to transmit a message to a given collection of receivers in an online setting, namely, when the hosts do not know each other's locations. The goal is to specify a protocol for the sender allowing it to directly broadcast the message to the recipients and receive acknowledgements, while minimizing the total transmission costs. By *direct broadcast* we mean that the sender is required to transmit the message itself to every recipient, namely, multi-hop delivery is not allowed. This restriction may be relevant in situations when the battery resources of the receivers is severely limited and it is desired to minimize their transmissions, or when when the reliability of the hosts is uncertain and only direct messages from the source can be trusted. Using varying levels of transmission power is important for energy-efficient communication. As far as the authors are aware, there has been no online algorithms with provable worst-case guarantees for energy-efficient broadcasting in ad-hoc wireless networks. The protocols proposed in this paper are based on computing or estimating the distances from the sender host to the receiver hosts in an energy-efficient way. The most basic case is that of a single sender and a single receiver. The generic doubling protocol employed by the sender is based on repeatedly transmitting the messages to increasingly larger distances, until reaching the receiver. The behavior of this protocol depends on the choice of the sequence of distances, and the problem is to determine them so as to minimize the overall power consumption. If a specific probability distribution may be assumed on the hosts, the algorithm can be optimized. This paper, however, assumes an online setting in which no a priori information is given about the distance from the sender to the receiver. Therefore the worst-case scenario should be considered. This motivation leads us to apply a competitive analysis to the algorithm. We compare the power consumption of an algorithm with that of the optimal (infeasible) offline algorithm that knows the distance d. We show that the optimal competitive ratio for this problem is $3/2 + \sqrt{2}$, i.e., there exists an online algorithm for the problem with this competitive ratio, and no online algorithm has smaller competitive ratio. The problem is somewhat similar to the famous *cow path* online problem, but setting the parameter of the algorithm is not obvious. Furthermore, we study the generalization of this problem where there is more than one receiver. This is a propoer extension of the cow path problem. For this problem we also propose a competitive online algorithm and prove its optimality. Interestingly, the competitive ratio of the generalized problem is the same, namely, $3/2 + \sqrt{2}$.

6. V. Mäkinen, G. Navarro, K. Sadakane: "Advantages of Backward Searching — Efficient Secondary Memory and Distributed Implementation of Compressed Suffix Arrays", Proceedings of ISAAC, LNCS 3341, 681–602, Dec. 2004.
概要: One of the most relevant succinct suffix array proposals in the literature is the Compressed Suffix Array (CSA) of Sadakane [ISAAC 2000]. The CSA needs $n(H_0 + O(\log\log\sigma))$ bits of space, where n is the text size, σ is the alphabet size, and H_0 the zero-order entropy of the text. The number of occurrences of a pattern of length m can be computed in $O(m \log n)$ time. Most notably, the CSA does not need the text separately available to operate. The CSA simulates a binary search over the suffix array, where the query is

compared against text substrings. These are extracted from the same CSA by following irregular access patterns over the structure. Sadakane [SODA 2002] has proposed using *backward searching* on the CSA in similar fashion as the FM-index of Ferragina and Manzini [FOCS 2000]. He has shown that the CSA can be searched in $O(m)$ time whenever $\sigma = O(\text{polylog}(n))$. In this paper we consider some other consequences of backward searching applied to CSA. The most remarkable one is that we do not need, unlike all previous proposals, any complicated sub-linear structures based on the four-Russians technique (such as constant time *rank* and *select* queries on bit arrays). We show that sampling and compression are enough to achieve $O(m \log n)$ query time using less space than the original structure. It is also possible to trade structure space for search time. Furthermore, the regular access pattern of backward searching permits an efficient secondary memory implementation, so that the search can be done with $O(m \log_B n)$ disk accesses, being B the disk block size. Finally, it permits a distributed implementation with optimal speedup and negligible communication effort.

研究会等

1. 定兼 邦彦:
“圧縮全文索引構築アルゴリズムの実験的評価”, コンピュテーション研究会, COMP2004-50, 47–54, 2004 年 10 月.
概要: 圧縮全文索引は文字列に対する索引であり任意のパタンを高速に検索できる．そのサイズは一般に元の文字列よりも小さくなるが，索引の作成時には大量のスペースが必要であった．本稿では近年提案された省スペースな索引構築アルゴリズム 3 つを実装し，実行速度，必要メモリに関する実験を行う．

2. 伊川洋平, 定兼邦彦:
“ホットリンク解析によるサイト内検索エンジンのランキング改善手法 大規模な Web サイトへの適用と考察”, データ工学ワークショップ, 1C-o2, 2005 年 3 月.
概要: Web 検索エンジンの利便性を向上させる手段として，ハイパーリンクを解析し，各 Web ページの重要度に応じてスコアを割り当てるスコアリング技術が重要視されている．WWW 検索エンジンのためのスコアリング手法は広く研究されているが，サイト内検索エンジンのためのスコアリング手法は未だ確立しておらず，Web の大きな特徴であるリンク情報を活用できていないのが現状である．この点に着目して提案された，ホットリンクを用いたスコアリング手法は，ユーザーが特定のコンテンツへ直接ジャンプできるように設定するホットリンクを分析することで，重要なコンテンツページに高スコアを割当て，サイト内検索エンジンのランキングを改善する手法である．本手法は，これまで小規模な Web サイトにおいて有効性が検証されているが，大規模な Web サイトについては充分検証が行われていなかった．本論文では，本手法が大規模な Web サイト対しても，重要なコンテンツページに高スコアを割当てることを実験により確認し，サイト内検索エンジンにおいて有用なスコアリング手法であることを検証する．

学会大会等

1. 後藤隆元, 小野廣隆, 定兼邦彦, 山下雅史:
“文書データベースへの効率的な索引付けとその更新に関する研究”, 火の国情報シンポジウム, B-1-6, 2005 年 3 月.

3.　各種資料

特定領域研究
「新世代の計算限界」ニュースレター　　第 1 号　　2004/11/5

はじめに

このニュースレターは，特定領域・新世代の計算限界のメンバーの情報交換と交流を目的とした情報発信誌です．毎回，いくつかの研究関連の記事と，特定領域のスケジュール・活動報告と，各研究者の活動予定などをお送りいたします．

各号は電子メールで配布する予定です．短い記事や連絡事項は全て掲載しますが，長い記事，イベントの詳細などは web ページに掲載する予定です．web ページには詳細まで全てを載せた完全版を掲載して，目次，あるいは各記事の末尾の URL を参照すると，web 版の同じ記事を参照できるようにいたします．

記事は，各回，1つの研究課題に担当をお願いする予定です．各研究課題で 2000-4000 字程度，研究に関わる記事を書いていただければと思います．通常，このようなニュースレターでは，研究成果を報告するのが一般的だと思われますが，この特定領域では「研究者の交流」に焦点を当てたいため，「研究の成果以外」の記事を面白く解説していただければと思います．例えば，最近参加した国際会議の情報を，どのようなものが流行っていたか，何が面白かったか，などの主観的な解説を交えて報告をしたり，最近考えている問題，あるいはオープン問題を，この辺までは解けるがここがうまくいかない，といった解説を交えて紹介する，という形です．

また，研究者間の交流を促進するため，各研究者の，国内外の会議への出席予定を集約して掲載していこうと考えています．研究者の交流には，顔をあわせる回数を増やすことが肝要です．他の研究者の参加予定がわかれば，会議への出席のモチベーションを高めることにもつながり，それがディスカッションや研究成果を生むきっかけにもなるでしょう．特定領域メンバーの皆さんには，自分のわかる範囲で，国内外の会議・研究会の情報と，自分の参加予定を教えていただければと思います．

この他，個人からの寄稿を募集いたします．100-1000 字程度で，情報宣伝されたいことを自由な形式で書いて送っていただければ，掲載いたします．メールで配布する関係上，テキスト形式のものしか扱えませんが，そこはご了解お願いいたします．

★ ニュースレター編集委員では，皆様からのご意見をお待ちしております．編集方針や内容の追加など編集全体にかかわることから細かいことまで，幅広いご意見をお願いいたします．

■■ 新世代の計算限界 ニュースレター ■■
編集委員長 宇野 毅明 uno@nii.jp (問合せ先)
副編集委員長 牧野 和久 makino@sflab.sys.es.osaka-u.ac.jp

第 1 号:　目次

1. 特定研究「新世代の計算限界」のスタートに当って　－ 岩間 一雄 (京都大)
2. 特定領域研究「新世代の計算限界」の発足を祝う　－ 稲垣 康善 (愛知県立大)
3. 寄稿：An introduction to the puzzle of European research funding　－ Josep Diaz (スペイン・カタロニア工科大学)
4. 2004 年度第2回幹事会・第1回全体討論概要　－ 事務局
5. イベントカレンダー

特定研究「新世代の計算限界」のスタートに当って

京都大学　岩間　一雄

アテネ五輪では思わず興奮してしまった諸兄も多いと思われるが，一段落して落ち着いて来ると色々と見えてくる．私が注目したのが競技（陸上，競泳，野球等）と種目（男子100メートル競争等）である．全体では種目の数は結構
膨大で300にも上るらしいが，勿論「格」の違いがはっきりしている．例えば陸上の中でも，マラソンは「五輪の花」でそれを制した野口選手の偉大さは（こういう言い方は良くないが）繰り上げ金メダルの室伏選手とは比較にならない．このことは選手自身も良く理解しているらしい．だからこそ，末続選手は去年の世界選手権では200メートルでメダルを取っているのに今回は100メートルに挑戦したが，全く歯がたたなかった．競泳で2個の金メダルと騒がれた北島選手であるが，平泳ぎである．柴田選手の自由形の快挙と比べるとどうなのであろうか．（ただ，米国のマスコミでは北島選手は大きく取り上げられていた．例の泳法違反の疑いの件ではあるが．）

しかしなんだかんだ言ってもオリンピックの競技でメダルを取ることは文句無しに偉い．心ならずも貶してしまったが，ハンマー投げは技術力がものを言うという希有な種目で私自身大好きである．格云々とは言っても，オリンピックに入っているだけで十分にすごいし，比較的「楽な」種目で勝つことは賢い人の常套手段である．更には，「入れてもらえない」スポーツも数多く存在するのである．例えば相撲は，その勝敗の分かり易さという点では格闘技の中でもピカーであるが，残念ながら例の褌の問題でもうひとつ世界に普及しない（その代り日本の大相撲が世界の中心になりつつあるのでまあいいか．）スケートボード，ローラースケート，サーフィン（開催場所が難しいか．．．）などなどの愛好者の数は一部のオリンピック競技（具体的には言わないが）よりははるかに多いと思われる．ただ，良く見ると，「入れてもらっている」競技にしてもその扱いは公平ではない．例えば，柔道だけで男女合わせて14個も金メダルがあるのに，野球やソフトボールはあんなに長丁場の試合をして，金メダルの個数は「1個」である．国別メダルの獲得競争で，野球なら9個とまでは行かなくとも5個くらいに換算してあげても良いのではないだろうか（あるいは体操の種目別のように首位打者や本塁打王も表彰するとか）．まあ，スポーツにもある種の政治が絡むのは常識であるが，幸運にも私は当事者ではない．自らに直接関係無いこうした「力関係の妙」を見るのは本当に楽しいものである．

暢気なことを言っている場合ではない．我々学者の世界だって典型的な競争と（複雑かつ微妙な）力関係の社会なのである．ちなみに私や本特定研究の参加者の多くは大きな括りでは「情報学」（名称に関しては色々御意見があろうかと思うがここでは議論しない）に属している．10年くらい前までは工学の中の一分野に過ぎなかったが昇格したのは大変喜ばしい．同じレベルの分類で言えば，物理学，経済学，医学，といった辺りが来るのであろう．過去数十年では，明らかに最も発展した学問分野であることは間違いない．特定領域でも，総元締の「ITの進化の基盤を拓く情報学研究」を始め，データマイニング，分子計算，といった幾つかの領域が走っていて優遇されている．しかし，上には上もあるのである．例えば，お医者さんの世界はけた違いにすごい．大雑把に言えば科研費全体のおよそ半分が医学とその関連分野に流れているのである．特定研究でも，我々の10倍以上の50ー100億といったプロジェクトが目白押しである．それらのいくつかは，「予定されている」ものらしく，ほぼ同じタイトルで5年おきに更新されていく．物性関係や宇宙も非常に強い．「ナノ・・・」というタイトルがいくつも目につく．実験系の物理がお金を食うのは分かる．最近量子計算で物理の先生のお話を伺うチャンスも多いが，極端な話，お金＝業績というケースも多いらしい．医学も実験が大変らしい．実験動物の値段を聞かされてびっくりした事がある．まあ，しかし総合的に見れば，我々の分野は「入れてもらっている」方になるのであろう．有難いことである．

次に情報学内部の「種目」を見てみよう．我々はアルゴリズムと計算量ということで，大雑把に言えば基礎理論である．さて，威張れるのであろうか．ひとつの尺度として，大学の情報関係学科における我々の仲間の占める割合を見てみよう．まず，天下のMITとStanfordであるが，双方とも計算機科学科の先生の数は50名程度である．その内で，理論の人は12ー3名といったところである．（但し，数学科所属の人もいるので注意．例えばMITでは，Goemans,Leighton, Shor, Sipserといって蒼々たる顔触れが上のカウントには入っていない．）大雑把に言えば，全体のおよそ25％が理論と言った感じになる．ただし，同様に大御所であるCMUは雰囲気が違って，この数字がおよそ1割に落ちる．わが国に目を向けてみよう．私の地元の京大

であるが，母集団をどこに取るかが難しいのであるが，例えば情報学研究科の教員数はおよそ 130 名程度である．半分強を情報関係と見れば約 70 名，その内の理論は 7ー8 名という感じである．つまり CMU と同じ 1 割である．この 1 割というのがわが国における標準的数字では無いかと思う．京都の場合は母集団が比較的大きいので恵まれている（建築に加藤先生，数解研に藤重先生もおられる）．学内の理論計算機グループの研究会である kids は先日第 19 回目のミーティングを行うことが出来た．この 1 割を（一部の大学であったとしても）MIT なみの 2 割 5 部まで上げることができないだろうか．私の大きな夢である．

学会はどうであろうか．ACM のチューリング賞は 40 回以上になるが，理論がおよそ25%と言ったところである．ACM の会長に関しては過去のデータが見つからなかったが，昨年度の会長はあの Maria Klawe だった．わが国の情報処理学会の会長は現在まで 22 名を数えるが，理論関係では野口正一先生だけの様である．学会の役員は色々難しい事情もあるのだろうが，大学の要職に目を向けると目を見張るものがある．まず，野口先生は会津大学の学長も経験されている．本多波雄先生は豊橋技術科学大学の学長をなさっている．木村正行先生は北陸先端科学技術大学院大学の，有川節夫先生は九州大学の，都倉信樹先生も鳥取環境大学のそれぞれ副学長をなさっている．更に学部長・研究科長では最近だけでも稲垣康善，上林彌彦，茨木俊秀，丸岡章の各先生が就任されている（他にもいらっしゃると思いますが思いつかず，申し訳ございません）．こうして見ていくと，理論分野の大先輩のご活躍は本当に立派で我々の大いなる誇りである．

更に理論分野の中の小分類（研究テーマ）を見てみよう．陸上のハンマー投げとマラソンでは違いが大きすぎて途中から転向するなど思いもよらないだろうが，我々の研究テーマの間にはそれほどの壁は無い．実際，多くの仲間が多かれ少なかれテーマ変遷の歴史を持っていると思われる．私自身も 45 才のころに（偶発的な事情から）量子計算を始めることになった．力不足で私自身の到達度は未だ心もとない状態ではあるが，本当に得難い経験をさせてもらった．議論の展開を式の流れ中心で進めて行くという流儀に出会い，世の中にはこの方がずっと解りやすい人が多くいることに感動した．フーリエ変換なるものがやっと解った（ような気がした）のも量子計算のお陰である．理論分野を 2 つに大別するとすれば，計算量理論とアルゴリズムであろうが，これら 2 つの間を渡り歩いた人も多く存在する．例えば，本特定研究の評価委員を御願いした Josep Diaz は構造的計算量理論の教科書を書いているが，現在はアルゴリズム中心の人である．ただ，彼も言っているように，計算量理論でも基本テクニックは勿論「アルゴリズム」であって，その意味ではこのような分類自体が意味を成さないのかもしれない．何度も言っているように，我々の分野は十分恵まれているのであって，研究テーマの選択は贅沢な悩みかもしれない．だからといって何でもうまく行くのではないことも又当たり前で，その微妙なところが（運も重なって）成功と失敗の分かれ目にさえなりうる．曰く言い難しとはこのことであろう．

最後になってしまったが，本特定領域の準備段階では多くの皆様から筆舌に尽し難いご援助を賜った．特に，申請書を書く時のタイトル，基本ポリシーについて議論したときは，私自身の今までの取り組みの浅はかさを痛感させられてしまった（いつの頃からか盲目的に人気のあるテーマに追従するという姿勢になってしまっていた）．多くの諸兄が全く反対の，理論とはこうあるべきだ，我々のコミュニティの発展のためにはこうしなくていけない，といった固い信念を持って日々の研究に取り組んでいることを知って驚く（失礼！）と共に大いに力付けられた．これなら，本プロジェクトの成功は間違いないであろうと確信するに至った．医学分野のように，次々とプロジェクトを連続させることが出来るようにしたいというのが今の私の最大の願望である．

特定領域研究「新世代の計算限界」の発足を祝う

愛知県立大学　稲垣 康善

本特定領域研究の代表者の岩間先生から，「大分以前になりますが，来年度発足を目指して科学研究費の特定研究を準備していることをご連絡差し上げました．」という書き出しで始まる平成15年11月19日付けのお手紙とともに，文部科学省に提出の申請書1部をお送りいただいてから，1年になります．そのお手紙の中には，「今後も審査突破に向け，誠心誠意努力する所存でございますので･･･」とありました．その通りのご努力の結果，この度，本研究領域が発足する運びとなりましたことは，我が国のコンピュータサイ

エンスの発展にとって誠に喜ばしく，お祝い申し上げる次第です．

岩間先生からのお送りいただいた申請書を拝見し，本研究プロジェクトは離散的アルゴリズムの分野で，厳密に正しい解を計算することが原理的に困難な問題に対してもコンピュータ利用が盛んになり，その結果，従来の計算効率による評価から計算結果の品質の良さにアルゴリズムの評価の中心が移り，そのことによって従来考えられてきたフィージビリティの限界を超える新しいアルゴリズム開発が次々と行われるようになったとの認識に立ち，新しいアルゴリズム研究の指針を確立しようと言う挑戦であると理解しました．総括班のもとに27の研究項目が設定され，いずれも現在の重要な研究課題であると頼もしく読みました．

昨2003年，ACMの50周年記念のJACMが発行されましたが，コンピュータサイエンスも半世紀を超える歴史を重ねるまでになりました．私事で恐縮ですが，私は1962年に名古屋大学の電子工学科を卒業して大学院に進学し，それ以来オートマトンと言語の理論と，それをよりどころにした研究をしてきました．計算可能性の理論から出発し，形式的モデルと意味論，アルゴリズムと複雑さの理論にいたる，コンピュータサイエンスの基礎理論の発展の歴史の中でこれまで勉強を続けてこられたことを幸いに思っています．

振り返ってみますと，シャノンの情報量の定義は，情報の科学の発展に本質的な貢献をしました．情報の量を計ることができるようになったことは，情報を早く大量にそして間違いなく伝送することに関する技術を驚異的と言って良いほどに進めたと思います．引いてはコンピュータの技術はもちろん音声処理や画像処理の技術が進み，通信とコンピュータの技術が結合し，インターネットに象徴されるITの時代に至っていると思います．

一方，計算の複雑さを計ること，これは，オートマトン・言語理論を基礎に，その理論が築かれました．その結果，アルゴリズムの理論は大きく発展しましました．アルゴリズムを計算の効率の視点から客観的ないしは理論的に評価できるようになったことは，それは大きな力を発揮しました．現代のアルゴリズム研究の基礎を支えています．もちろんNP問題のように，数学的にもコンピュータサイエンス的にも興味深い，挑戦的な課題も残されていますが，
実用的な観点からは，アルゴリズムの解析と設計に関して実に多くの成果を人類の手の中にもたらしました．

その結果，易しい問題，困難な問題を見極めることができるようになり，また，どの程度の難しさであるかを言うことができるようになりました．困難な問題であると分かっても，難しいからと言って手をこまねいているわけにもいかず，解の精度や確度をも評価にいれ，種々の意味で近似的に解を求める理論と技術に関する研究が盛んです．シャノンの情報理論が実用に結びつくなかで，歪み理論が重要であったように，解の品質が評価の基準に据えられるようになってきているのは，アルゴリズムの理論が広く実用に役立てる状況に，そしてその時期にきていると思われます．

このようなときに，我が国のこの分野の先導的な最も優れた研究者が集まり，本特定領域研究が発足したことは，大変に意義深いことと思います．茨木先生のアルゴリズム工学に関する特定領域研究に続きこの分野の更なる発展に貢献されることはもちろん，新しいフロンティアを開拓されることを期待しています．さらに，この領域研究が，それだけにとどまらず，国内外の多くの研究者の参加も得て，我が国のコンピュータサイエンス分野の研究の発展の為に，そして，国際的にも，大いなる貢献を期待しています．

簡単ではありますが，これをもって，本研究領域研究に参加し研究を推進される研究者の皆様の大いなる活躍を祈りつつ，本特定領域研究発足に際してのお祝の言葉といたします．

寄稿：An introduction to the puzzle of European research funding

Josep Diaz (スペイン・カタロニア工科大学)

At the end of the decade of the 70's, the European Union (EU) decided to invest in order to create strong research groups formed with teams from different EUcountries. The research Framework Programmes were created. They coexisted and rely on the national research programmes from each EU country.

Before continuing, we need a little explanation of the political setting of the EU. The EU has the European Parliament, elected by the citizens of the EU countries, and the European Commission, nominated by the governments of the different EU countries (*1). The European Commission has 17 *general directorates* (GD) equivalent to ministries, among other the *GD of Information Society*, the *GD of*

Research and the *GD of Energy and Transport*. The research founded by the Framework Programmes was spread (and still is) among different (GD), in particular the ones mentioned above.

In 2000, there was the convincement in the European Commission, that the lack of coordination between EU Framework Programmes and the programmes of individual countries resulted in a duplication of effort and dissipation of resources, which made difficult to talk about European research as a coherent entity, in the same way that we could talk about Americanor Japanese research. Therefore, in order to make the European Union one of the most competitive and dynamic knowledge-based economy in the world by 2010, the European Union established the concept of *The European Research Area* (ERA), which is intended to be a legislative framework for developing at the European level a joint and coordinate research effort, which will create an European critical mass of researchers in different fields, and hopefully would attract the best researchers from the rest of the world.

The main instrument to start implementing the ERA concept was the *6th Framework Program* (FP) (2003-2007). In the words of the official advertisement of the European Commission (EC) *"the FP6 will channel its budget into actions and projects designed to build the ERA in partnership with Europe's best researchers"*. The FP6, still coexists with national programs, but the amount of resources dedicated are greatly increased with respect to the previous FP, which in some cases implies that some EU countries had to make drastic cuts in their national programmes. In the FP6, the research is focused on specific themes that are strategically important to Europe's future (according to the European Commission). They are not structured from the starting point of traditional research disciplines. The FP6 priority themes are the following (among parenthesis the millions of Euros devoted to each priority):

1. Life sciences, genomics and biotechnology for health (5028)
2. Information Society Technologies (IST) (3984)
3. Nanotechnologies and nanosciences, knowledge-based multifunctional materials, and new production processes and devices (1429)
4. Aeronautics and space (1182)
5. Food quality and safety (753)
6. Sustainable development, global change, and ecosystems (2329)
7. Citizens and governance in a knowledge-based society (247).

There are other source of founds within FP6, for instance support to big European infraestruture (like an European GRID) (715), the Euroatom program (1230), international cooperation (developing countries, Latin America and other joint programs like with NSF) (401), and others. The most relevant priority area to this report is the *Information Society Technologies* (IST), which fellin the DG 11, Information Society. The IST is subdivided into four subprograms:

1. Applied IST research addressing major social and economical challenges.
2. Components and Microsystems.
3. Communication, computing and software technologies.
4. Knowledge and Interface technologies.

Each one of those has a budget of 896 millions of euros. There are three modalities of projects inside of each program: The *network of excellence* large teams of researchers from EC countries or associate states form a network for traveling, (within Europe), holding workshops and schools, interchange of students and researchers, etc. At the moment there is one such a network per subprogram. The Integrated Project, rather large projects, with substantial participation of industrial partners (mandatory) designed to create the knowledge required to implement a new result in the area, which is achieved by integrating a critical mass of activities (research, demonstration, training, innovation, management) and resources (staff, skills, competences, finances, infrastructure, equipment etc.). The IP get the largest share of the budget. The third modality is the *Specific Targeted Research Projects* (STREP), small size projects where the goal is developing new products or processes contributing to meet the needs of society or community policies (this could be considered more academic projects with limited number of partners and a focused goal).

Moreover, in IST there is a fifth subprogram: *Future and Enabling Technologies* (FET), which is the subprogram corresponding to basic research. It has a budget of 400 millions of euros. There are two kinds of projects, the *Open scheme* and the *roactive initiatives*. The purpose of FET open is to enable a range of ideas for future and emerging technologies to be explored and realized. The scheme is open to the widest possible spectrum of research opportunities that relate to Information Society Technologies. There are STREP type and the usual budget is around 2.5 millions euros for 3 years and 10 partners. The partners must be at least from 4 different countries of the EU or associated states. Trips outside Europe must be very detailed justified.

On the other hand, the proactive initiatives are launched on topics where early ground breaking work has already demonstrated an important potential, but where significant scientific or technological barriers and risk justify a concerted action at basic research level before the area can be taken up as mainstream industrial research. The initiatives usually involve multidisciplinary work at the frontier of information technology. The total budget per initiative inacallmay be in the range of 15 to 30 million euro, and can be covered by several projects (around 4 or 5 different projects have been approved for each proactive initiative). Some of the recent initiatives are: *Global Computing, Bio-Inspired Intelligent Information Systems, Quantum Information Processing and Communication, Complex Systems, and The Disappearing Computer*. For an example of a project in the Complex System initiative see the web page http://delis.upb.de/. The great drawback of the projects is he great amount of paperwork involved (directly proportional to the founding amount). I have no experience outside FET, but I guess in other subprograms, the burocratic load must be quite heavy. Other kinds of support are the *Marie-Curie scholarships*, where a researchers (from a EU country or associated state) apply for a scholarship to be during 4 years in a given university (in the EU).

ALCOM: A case of study

In 1988, eleven teams working in algorithms in Europe asked for a project to develop the field of Algorithms and Complexity in Europe. The project was awarded and started in May of 1989, with a global budget of 1.5 Million euros. The participant sites were Aarhus Universitet, Computer Technology Institute (Patras), EHESS-CAMS (Paris), Frei Universitaet Berlin, INRIA-Paris, INRIA-Sophia-Antipolis, Max Planck Institut fur Informatik, UPC, Universita di Roma "La Sapienza", Universiteit van Utrecht, University of Warwick. Fourteen years later ALCOM-FT (the 4th. ALCOM founded by the EC) finished. The project had a budget of 2.5 million euros for 4 years, and the participants in that ALCOM were: Aarhus Universitaet, Computer Technology Institute (Patras), INRIA-Paris, Max Planck Institut fur Informatik, UPC, Universitaet zu Koln, Universita di Roma "La Sapienza", University of Cyprus, Universitaet zu Paderborn, Universiteit van Utrecht, University of Warwick. Behind there is a history of over 60 successful theoretical Computer Scientist trained by the ALCOM projects, which hold academic (many of them at the Professor level) and industry positions in Europe and elsewhere (even one of them in Japan). Over 1000 published papers and books, several computer systems, the better known LEDA and ABACUS. It is beyond any doubt that the ALCOM series played an key role in the development of algorithmics in Europe, and it has been crucial in the scientific and human development of the author of this report.

(*1) At this moment there is a very hot issue about the way the Commission is selected. The Commission is the executive body of the EU, which proposes initiatives, and the Parliament is the legislative body which approves of rejects the commission initiatives. The composition must be ratified by the parliament, and the actual parliament has demanded changes in the composition of the new Commission before ratifying it.

2004 年度第2回幹事会・第1回全体討論概要　　事務局

日時: 2004.10.13, 幹事会: 12:00--13:40, 全体討論: 16:15 -- 17:30
場所: 東北大学 工学部 電気情報・物理工学科,
幹事会: 1 号館 4 階 451・453 大会議室
全体討論: 講義棟 1 階 103 号室
出席者:
幹事会: 浅野孝夫, 浅野哲夫, 宇野毅明, 加藤直樹, 櫻井幸一, 瀧本英二,
徳山 豪, 西関隆夫, 林 幸雄(学術調査官), 渡辺 治,
岩間一雄, 伊藤大雄, 堀山 貴史
全体討論: 省略

○学術調査官の林先生の評価コメント
・ 情報分野の基盤を支える研究であり, 高い国際競争力を期待する.
・ 現実問題を対象として従来の理論では解明できないものを解明していくための新しいパラダイムを期待する.
・ 領域全体としてどういう成果が出るかが問われる. 連携, 総括班が重要.
・ 品質評価について, 基準, 目標が不明確.
・ 計画の具体性, マイルストーンが必要ではないか.
・ 個別研究班の申請に対し幾つかの問題点が指摘された.
・ 中間審査が 2005 年の9月ごろにある.

○一般向け雑誌と教科書シリーズ
・ 一般向けの雑誌 … サイエンス社 不可能ではない (渡辺先生)
・ 教科書シリーズ … 共立出版 前向き (山下先生, 杉原先生)
・ 来年9月の中間審査までに
- 雑誌の出版
- 教科書シリーズの青写真
を間に合わせたい.
・ 渡辺先生, 山下先生, 杉原先生に継続して舵取りを依頼

○ジャーナル
・ 外国の雑誌に貢献しているが, 日本からの情報発信が必要.
・ 電子ジャーナルを主に考えている.
・ 継続性や存在価値など色々検討すべき点も多い.
・ 継続審議(調整役:徳山先生)

○キックオフ国際会議
・ 会議名称:International Symposium on Recent Trends in Compter Science
・ 2005/2/28(月) ～ 3/3(木), 京都ロイヤルホテル
・ PC co-Chairs: 徳山先生, Magnus 先生
・ 発表は全て招待講演で, 20 件の発表を予定
- 呼んでほしい人がいれば, 徳山先生にメールで.
(運賃と講演料等は総括班で補助できる.)

○日洪シンポジウム
・ 2005/6/3(金)--6(月), ブダペスト
・ 学生のハンガリーへの渡航補助を行う.

○特定「確率的情報処理」(略称 SMAPIP)とのジョイントのシンポジウム
・ 2005/7/18(月)--21(木), 仙台国際センター
- 19,20: 計算限界主体, 20,21: 確率的情報処理主体
(ただし, 20,21 には両特定領域の交流の場となるような構成とする)
・ 依頼講演のみ
・ 計算限界側担当者:渡辺治先生, 松井知己先生.

○研究集会の推奨

・ 総括班から補助をするので，特定のメンバー全員が一度は集会を組織するつもりで，どんどん申し出て欲しい．どんな若手でも遠慮は全く無用．

・ 事務局から直接，組織をお願いする場合もあるのでご協力下さい．

○ニューズレター

・ 年に 3 ～ 4 回，持ち回りで研究成果以外の記事を書くなどして，研究者同士の交流をすすめる．

・ 編集委員長：宇野先生，副委員長：牧野先生

○招聘研究者，PostDoc 研究員

・ 招聘研究者を呼びたい場合は遠慮なくご相談ください．なるべく総括班から補助を出すようにします．

○今後の全体会議

・ 基本的に半年に1回の開催とする．

・ 次回は2月に国際会議があるので，5月とする（二日間）．

・ 場所は東京電機大学（築地先生が世話役）［注：全体討論の時から変更有り］

「新世代の計算限界」イベントカレンダー

■ 2004 年 ■

11/5(金) アルゴリズム研究会，愛知県立大
http://www.hirata.nuee.nagoya-u.ac.jp/sigal/

12/10(金) コンピューテーション研究会，東邦大
http://tcslab.csce.kyushu-u.ac.jp/COMP/

12/20(月)-22(水) ISAAC，香港
http://www.cs.ust.hk/~isaac04/

■ 2005 年 ■

1/23(日)-25(火) SODA，バンクーバー
http://www.siam.org/meetings/DA05/

1/31(月)-2/2(水) 冬の LA，京大数理解析研
http://la.is.nagoya-u.ac.jp/

1 月 アルゴリズム研究会，東京
http://www.hirata.nuee.nagoya-u.ac.jp/sigal/

1 月 コンピューテーション研究会，名古屋大
http://tcslab.csce.kyushu-u.ac.jp/COMP/

2/28(月)-3/3(木) キックオフ国際会議

3 月 コンピューテーション研究会，東工大（2 日間）
http://tcslab.csce.kyushu-u.ac.jp/COMP/

3 月 アルゴリズム研究会，東京
http://www.hirata.nuee.nagoya-u.ac.jp/sigal/

5/21(土)-24(火) STOC，バルチモア
http://www.cs.jhu.edu/~stoc05/

6/3(金)-6(月) 第 4 回日洪シンポジウム

7 月 確率アルゴリズムの合同シンポジウム

特定領域研究
「新世代の計算限界」ニュースレター　　第 2 号　　2005/3/8

このニュースレターは，特定領域・新世代の計算限界のメンバーの情報交換と交流を目的とした情報発信誌です．毎回，いくつかの研究関連の記事と，特定領域のスケジュール・活動報告と，各研究者の活動予定などをお送りいたします．

1. ボロノイ図とその応用国際シンポジウムを開催して　－ 杉原厚吉（東京大）
2. NHC Workshop Business Meeting (兼 2004 年度第3回幹事会) 議事録　－ 事務局
3. イベントカレンダー ＋ 事務連絡
4. このニュースレターについて

ボロノイ図とその応用国際シンポジウムを開催して

杉原厚吉（東京大学）

昨年 9 月に東大で International Symposium on Voronoi Diagrams in Science and Engineering (ボロノイ図とその応用国際シンポジウム) を開催した．3 日間で 24 件の発表があり，79 名の参加者を得た．そのうち海外からの参加者は 18 名であった．

ボロノイ図とは，いくつかの対象が，影響を及ぼす環境においてその影響の均衡を表す図形で，勢力圏図などともよばれている．影響力の与え方に多くのバリエーションがあり，それに応じてボロノイ図にも多くの変種がある．そして，その応用も多岐に渡る．このシンポジウムは，計算幾何の研究者と，応用分野の研究者がボロノイ図というキーワードを介して知見の交換をする機会を作ることを目的として開催された．

計算幾何にある程度なじんでいる人には，何でいまさらボロノイ図なのか，という疑問をもたれるかもしれない．実際，ボロノイ図は，計算幾何という学問分野が生まれた 1970 年代後半から 1980 年代前半にかけての主要なトピックの一つであり，もうずいぶん前に研究し尽くされた対象のように外からは見られがちである．

確かにアルゴリズムの理論家から見ると，ボロノイ図という畑の主要な果実はとっくに収穫され尽くされており，落穂拾いのようなドロ臭い話題しか残っていないように見えるだろう．主要な果実とは，アルゴリズム技法を華麗に駆使して，計算量を下げることのできる諸問題のことで，もう一方の落穂拾いとは，きれいな技では解決できず，ノウハウとか近似とかヒューリスティックとかいうきたない手をあれこれ尽くして何とか解らしきものが得られる問題のことである．

それにもかかわらず，この分野を取り上げて国際シンポジウムを開催したのは，応用の側から大きな要請や需要があると感じていたからである．

たとえば，有限要素法で使うメッシュを得るために，与えられた 3 次元領域を四面体に分割したいという要請（これはメッシュ生成とよばれる）がある．このとき有限要素解析の精度をあげるためには，四面体がなるべくふっくらとしていることが望ましい．2 次元領域を三角形に分割するときには，ボロノイ図の双対図形が，内角を小さい順に並べた列が辞書式順序で最大になるという意味の最適性をもつ．一方，3 次元のボロノイ図の双対図形では，そのような最適性は保証されない．しかし，ほかによい手があるわけでもないので，ボロノイ図の双対図形から出発して，いろいろな工夫を加味しながらなんとかそこそこよいメッシュを得ようとするのが一つの有望な方向である．これなどは，理論の立場から見ると，典型的な落穂拾いの課題であろう．

一般に，アルゴリズムを作るまでの道のりより，アルゴリズムを作ってからそれが実用に使われるまでの道のりの方が長いことが多いように思う．なぜなら，アルゴリズムを実際に使えるものにするという作業は，ソフトウェアへの単なる翻訳ではないからである．アルゴリズムを構成する段階では，最も重要なところを抽出して単純化した問題を対象とするのに対して，その成果を実用に供しようとすると，理論作りでは捨象した多くの制約や事情を考慮してアルゴリズムを変更しなければならない．そらに，誤差その他の外乱に対して安定に動作するロバスト性も確保しなければならない．その手間は一般に非常に大きい．

私の今までのいくつかの経験からは，アルゴリズムを作ったところで自分の役目は終わったとみなして，使いたい人はどうぞそれを勉強してプログラムにして自由に使って下さいと言っても，現場の人は誰も使ってはくれない．現場では，次々とこなすべき仕事があって，勉強に十分な時間がとれなかったり，たくさんあるアルゴリズム理論のどこをどう学べば自分の問題が解けるのかよく分からなかったりして，なかなか手を出してはもらえない．

したがって，自分の作ったアルゴリズムを本当に使ってもらいたかったら，こんな風に使えますよと，ある程度の例が示せるところまで，ソフトウェアを実装するところも，現実的制約を加味するところも，こちら側で面倒を見なければならない．しかしそのためには，現場の事情を理解するなどこちら側も時間を割いて勉強しなければならないから，それ相当の覚悟がいる．

これらのことを考えると，アルゴリズムの研究者にとって，自分の作ったアルゴリズムが実用に使われるまでの道のりのうち，どこまでを自分自身で面倒を見るべきかは大きな問題であろう．ここから先は，それぞれの研究者の人生観，主義などに関わるものであり，それぞれが自分で選択するしかない．理論体系の構築に精力を集中する立場から，現場にどっぷり浸かって最後まで見届ける立場までの中間にいろいろな立場があり得るだろう．

話をボロノイ図のシンポジウムに戻すと，そこで現場の需要に応える実用的成果がたくさん発表されたというわけではない．しかし，こんな問題にこんな風に使えそうですよと，研究者の側から応用を指向したメッセージはたくさん出されたと思っている．そこでの応用分野は，メッシュ生成，分子の立体構造の解析，画像や立体形状のデータ圧縮，データ補間，航路計画，パッキング，消費者行動のモデリング，スポーツのチームワーク解析など多岐に渡った．

詳しい内容を知りたい方には，シンポジウム論文集の残部があるので，杉原まで郵便住所をご連絡されたい．

また，日本応用数理学会公認英文誌 Japan Journal of International and Applied Mathematics (JJIAM) の第 22 巻 2 号 (2005 年 6 月発行予定) は，このシンポジウムの特集号として編集が進んでおり，10 編の論文が掲載される予定である．

なお，本シンポジウムは最初は 1 回限りのものとして企画したが，幸い年 1 回開催されるシリーズとして引き継いでいただいた．第 2 回目は，今年 (2005 年) 10 月 10 日から 13 日に韓国のソウルで開催される．また，来年の第 3 回は，スペイン，カナダ，アメリカ合衆国が誘地に名乗りを上げてある．

ボロノイ図という理論的には成熟した分野が，広範な応用の現場へ浸透していくのを支援する場として，このシンポジウムシリーズが役立つことを願っている．

NHC Workshop Business Meeting (兼 2004 年度第3回幹事会) 議事録　　事務局

日時:2005.03.02, 20:00--21:00
場所:京都ロイヤルホテル会議場(祥雲)
出席者:国際会議参加者より約40名(特定幹事, 招待講演者多数を含む)

海外からの招待講演者からの声を多く得ることを目的とし,
まず領域代表者よりプロジェクトの概要を説明し意見を求めた.
以下に主要な論点を記する.

・結果の出し方が重要，つまり科研費の成果の出し方は？
　どんな結果を出すと約束したか？
　　例えばこの会議が成功したと何を持って主張できるのか？など．

・この会議の招待講演主体というのは面白い試みである．
　新しいモデル，問題などの提案が多くあり，非常に有意義なものとなった．

・この会議で得られた情報を送ってくれれば
　まとめてデータベースを作っても良い（PCC より提案）．

・海外にも類似のプロジェクトがある．
　例えば ALADDIN PROJECT(http://www.aladdin.cs.cmu.edu/)は
　金額も目的も似ている．ただ，ALADDIN は年ごとに特定のトピックに
　限定して具体的な成果を出している．

・ヨーロッパのプロジェクトでは，1週間程度の期間，選ばれた学生を集めて，
　2～3のホットな話題に限定してスクールを行っている．
　これを行えばプロジェクトも継続する．

・日本の学生を海外の機関で2～3ヶ月面倒みてくれるか？→OK

・海外のプロジェクトと共同企画などは可能か？→可能

・本プロジェクトの成果に対して一部に楽観的な見方があるが，どうか？
　他の分野では（例えば OR などでも）具体的な成果をどんどん出している．

・教育や啓発（一般や高校生対象）も重要．

・雑誌や新聞などメディアの影響は大きい．

事務局まとめ：
今回の国際会議についてはたいへん好評であり，今後の継続に対する期待もあった．一方プロジェクト全体については，どう具体的な成果を出していくかが中心的な問題点として議論された．その中で，短期間のスクールによる学生の教育や，学生の交流，メディアを利用した啓発活動など，興味深い提案が得られた．また，話題を限定しての会議というのは，現在推奨しているミニ研究集会と一致しており，力づけられた．そして本プロジェクトに対して多くの海外の有力な研究者達が今後の協力を力強く約束してくれたことは，何よりも大きな成果と言える．

「新世代の計算限界」イベントカレンダー

★ ミニ集会，どんどん企画して下さい．楽しく活発に研究しましょう
★ 今年度の報告書をまとめます，3月末までに書いて下さい

成果報告書の執筆依頼

領域としての成果報告書を作成する時期となりました．A01 から C11 の
研究課題ごとに，「研究活動報告」と「発表文献リスト」を御執筆いただき，
原稿投稿のページより御提出いただけますようお願い申し上げます．
詳細は以下を御覧ください．提出〆切は 3 月 31 日(木) 午後5時です．
http://keisan-genkai.lab2.kuis.kyoto-u.ac.jp/members/reports.html

ミニ研究集会

JAIST ミニ集会「研究の種をいかに育てるか」 (浅野哲夫，上原隆平，元木光雄，Arijit Bishnu)
3/12(土) 10:00-17:00 JAIST 情報科学研究科 コラボレーションルーム

日大ミニ集会 (戸田 誠之助(田中圭介グループ))
chordal graph に関連した計算問題やアルゴリズムを中心に，講演と新たな課題探求に向けたディスカッションを行う予定です．
3/19(土) 10:00-17:30 日本大学・文理学部・8 号館1階レクチャーホール

列挙合宿 (宇野毅明・中野眞一)
3 日間、泊り込みで列挙アルゴリズムに関する雑談をします。
3/29(火)13:00 - 31(木)11:30 群馬県伊香保町 群馬大学セミナーハウス

3/17(木) アルゴ研，東芝科学館，川崎
3/18(金)-19(土) コンプ研，東工大(2 日間)， 招待講演 岩間一雄 (京大)
5/19(木)-20(金) アルゴ研・コンプ研連続開催，九州大
5/21(土)-24(火) STOC，バルチモア
6/6(月)-8(水) SoCG05，イタリア・ピサ
6/19(日)-23(木) SAT，イギリス・セントアンドリュース
6/22(火)-25(土) WG，フランス・メッツ 参加表明，宇野
7/11(月)-15(金) ICALP，ポルトガル・リスボン
7/11(月)-15(金) IFORS，ハワイ，
8/15(月)-17(水) WADS，カナダ・ウォータールー
8/16(火)-29(金) COCOON，中国・昆明
8/29(月)-9/2(金) MFCF，ポーランド・グダニスス
10/3(月)-6(木) ESA，スペイン・イビザ
12/19(月)-21(水) ISAAC，中国・海南島

このニュースレターについて

ニュースレター各号は電子メールで配布する予定です．短い記事や連絡事項は全て掲載しますが，長い記事，イベントの詳細などは web ページに掲載する予定です．web ページには詳細まで全てを載せた完全版を掲載して，目次，あるいは各記事の末尾の URL を参照すると，web 版の同じ記事を参照できるようにいたします．

記事は，各回，1つの研究課題に担当をお願いする予定です．各研究課題で 2000–4000 字程度，研究に関わる記事を書いていただければと思います．通常，このようなニュースレターでは，研究成果を報告するのが一般的だと思われますが，この特定領域では「研究者の交流」に焦点を当てたいため，「研究の成果以外」の記事を面白く解説していただければと思います．例えば，最近参加した国際会議の情報を，どのようなものが流行っていたか，何が面白かったか，などの主観的な解説を交えて報告したり，最近考えている問題，あるいはオープン問題を，この辺までは解けるがここがうまくいかない，といった解説を交えて紹介する，という形です．

また，研究者間の交流を促進するため，各研究者の，国内外の会議への出席予定を集約して掲載していこうと考えています．研究者の交流には，顔をあわせる回数を増やすことが肝要です．他の研究者の参加予定がわかれば，会議への出席のモチベーションを高めることにもつながり，それがディスカッションや研究成果を生むきっかけにもなるでしょう．特定領域メンバーの皆さんには，自分のわかる範囲で，国内外の会議・研究会の情報と，自分の参加予定を教えていただければと思います．

この他，個人からの寄稿を募集いたします．100–1000 字程度で，情報宣伝されたいことを自由な形式で書いて送っていただければ，掲載いたします．メールで配布する関係上，テキスト形式のものしか扱えませんが，そこはご了解お願いいたします．

★ ニュースレター編集委員では，皆様からのご意見をお待ちしております．編集方針や内容の追加など編集全体にかかわることから細かいことまで，幅広いご意見をお願いいたします．

■■ 新世代の計算限界 ニュースレター ■■

編集委員長 宇野 毅明 uno@nii.jp (問合せ先)
副編集委員長 牧野 和久 makino@sflab.sys.es.osaka-u.ac.jp

平成16年度 第1回 全体会議

日時　平成 16 年 10 月 13 日 (水)

会場　東北大学 工学部 電気情報・物理工学科 講義棟 1 階 103 号室

プログラム

12:00 – 13:40　幹事会

13:50 – 14:00　代表者挨拶

14:00 – 14:50　Approximation Algorithms for the Minmax Subtree Cover
永持 仁 教授 (京都大学 大学院 情報学研究科)

15:00 – 15:50　位相情報を用いた画像マッチングとその応用
— ピクセルとピクセルの間をみる技術 —
青木 孝文 教授 (東北大学 大学院 情報科学研究科)

16:15 – 17:30　全体会議

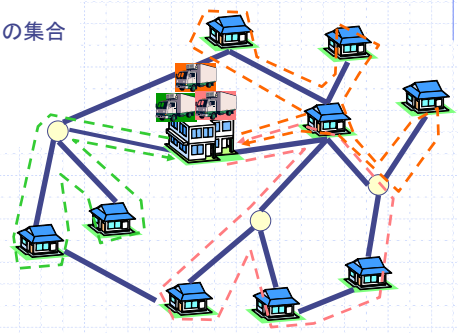
Approximation Algorithms for the Minmax Subtree Cover

Hiroshi Nagamochi
Kyoto University

グラフ上の配送経路問題

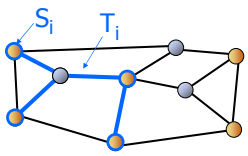
最大付加 (完了時間) を最小化

S: 訪問点の集合
r: デポ
p: 台数



Minmax Subtree Cover Problem (MSC)

入力: グラフ G=(V,E)，
枝重み w(e)，点重み h(v)
訪問点集合 S ⊆V,
整数 p ≧2



可能解: 分割 $\mathcal{S}=\{S_1, S_2, \ldots, S_p\}$ of S,
部分木の集合$\mathcal{T}=\{$ Ti （⊃ Si)| i=1,2,...,p}

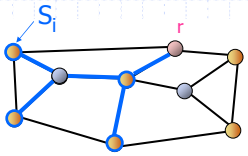
目的: Minimize
$cost(\mathcal{S},\mathcal{T}) \equiv \max\{ w(Ti) + h(Si) \mid i=1,2,\ldots,p\}$

$\Sigma\{ w(e) \mid e \in Ti\}$ $\Sigma\{ h(v) \mid v \in Si\}$

自然な問題設定だがこれまで研究例は少ない

Minmax Rooted Subtree Cover Problem (MRSC)

入力: グラフ G=(V,E)，
枝重み w(e)，点重み h(v)
訪問点集合 S ⊆V,
根 r
整数 p ≧2



可能解: 分割 $\mathcal{S}=\{S_1, S_2, \ldots, S_p\}$ of S,
部分木の集合$\mathcal{T}=\{$ Ti （⊃ Si+r)| i=1,2,...,p}

目的: Minimize
$cost(\mathcal{S},\mathcal{T}) \equiv \max\{ w(Ti) + h(Si) \mid i=1,2,\ldots,p\}$

$\Sigma\{ w(e) \mid e \in Ti\}$ $\Sigma\{ h(v) \mid v \in Si\}$

MSCに対する結果

MSC: NP-hard （S=V, h ≡0かつ G が木かメトリックでも）

	G: 木	G: 一般
S⊆V	(2-2/(p+1))-倍近似 O((p-1)! n) 時間 [Nagamochi, Okada 02]	（p=1のときSteiner木）
S=V	(2-2/(p+1))-倍近似 $O(p^2 n)$ 時間 [Nagamochi, Okada 03] (→ (4-4/(p+1))-倍近似 for a cactus G [Nagamochi, Kawada 04])	4-倍近似 O(m log n) 時間 h≡0 [Even, Garg, Konemann, Ravi, Sinha 04]

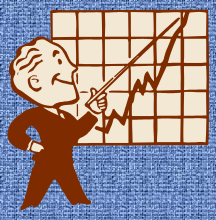
R. Hassinら，各成分Viの節点数niが指定，カット和最小化，
成分内の枝重み和最大化，G:metric

MRSCに対する結果

	G: 木	G: 一般
S⊆V	S=Vと仮定できる	
S=V	4/3-倍近似 (p=2) [Averbakh, Berman 96] (2+ε)-倍近似 $O(n \log \log_{1+\varepsilon/2} 3)$ 時間 [Nagamochi, Okada 03]	3-倍近似 O(mlog n) 時間 [Nagamochi 04] 4-倍近似 $O(m \log n + p^{2.5})$ 時間 R: 根の候補点集合， h≡0 [Even, Garg, Konemann, Ravi, Sinha 04]

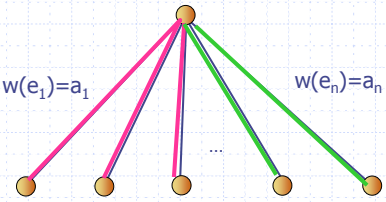
根からのk個の木でカバー，枝重み和最小化は２倍近似可能

I. Minmax Subtree Cover Problem (MSC)



木におけるMSC の例1

p=2, h(v)=0, v ∈S=V



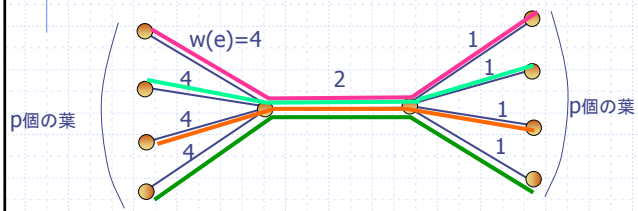
(PARTITIONと本質的に同じ)

木におけるMSC の例2

最適な部分木は枝素，点素とは限らない

h(v)=0, v ∈S=V

opt=7



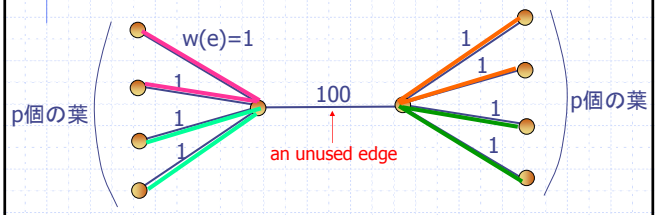
木におけるMSC の例3

w(T): Tの枝重み和

w(T)/p は下界とは限らない

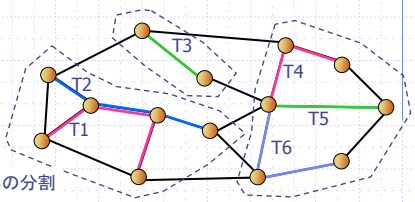
h(v)=0, v ∈S=V

opt=2 < w(T)/p



MSC に対する下界L(G,p)

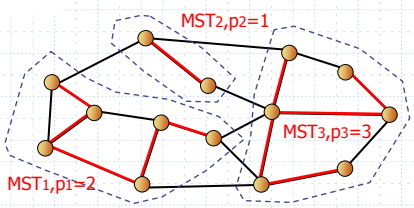
opt(G,p) ≧L(G,p)



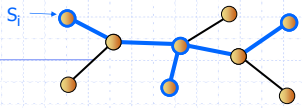
グラフのk個の連結成分への分割
V1,V2,…,Vk(1 ≦k≦p)
台数pの各成分への配分pi

MSTi：成分Viでの最小木
この分割パタン下での
コストの下界
$\max_i \frac{w(MST_i)+h(V_i)}{p_i}$

L(G,p):これをすべての
パタンで考えた最小値



木におけるMSC の性質



T[Si]: Siを含む極小な部分木

補題 1 [Nagamochi, Okada 02]
木において MSCの最適値optに対して
cost($\mathcal{S},\mathcal{T}$) ≦ max{ (2−2/(p+1))・L(G,p), max h(v)}
≦ (2-2/(p+1)) ・ opt
かつ
$\mathcal{T}$ = {T[S1], T[S2], …, T[Sp] }が辺素である
S ⊆ V の分割 $\mathcal{S}$={S1,S2,…,Sp} と部分木の集合$\mathcal{T}$ が
O((p−1)!n) 時間 で求まる.

``点素"に置き換えると cost($\mathcal{S},\mathcal{T}$)/opt は定数で抑えられない

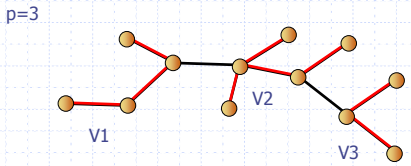
木の点素な部分木への分割

Lemma 2 [Perl, Vishkin 85]

$\mathcal{T}$={ T[V1], T[V2], …, T[Vp] }が点素となる

Vの分割 $\mathcal{S}$ ={V1,V2,…,Vp} で

cost($\mathcal{S}$,$\mathcal{T}$)最小のものがO(np(p+log n)) 時間で求まる.

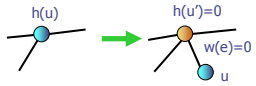


木の MSC に対する2倍近似アルゴリズム

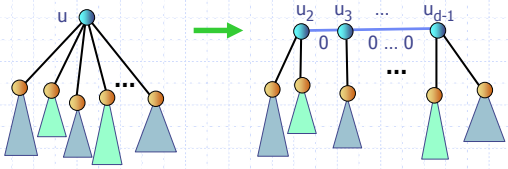
[Nagamochi, Okada 03]

入力: T=(V,E), S=V.

Step 1. 各葉 uに対し
新しい葉 u' を作る:



Step 2. 葉でない点 u を u2,u3,…,ud-1に分割:



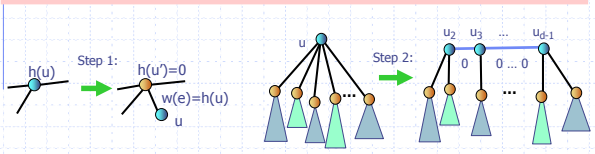
Step 3. minmax最適な点素なp個の部分木を求め,
これの誘導するVの分割を出力

正当性

Steps 1 and 2の後

(i) 最適性は保存

(ii) (2-2/(p+1))-倍近似で枝素な解がある(補題 1).
次数3以下であるので, 枝素は点素とみなせる



Step 3で

(iii) 点素でminmax最適な部分木集合はO(p^2n) 時間で得られる(補題 2).

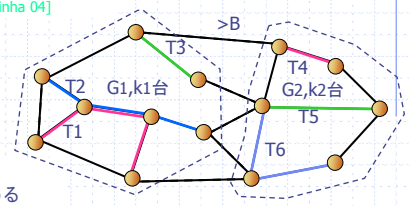
(iv) この点分割から得られる元の点分割は (2-2/(p+1))-倍近似. Q.E.D.

MSC に対する4倍近似アルゴリズム

[Even, Garg, Konemann, Ravi, Sinha 04]

h≡0

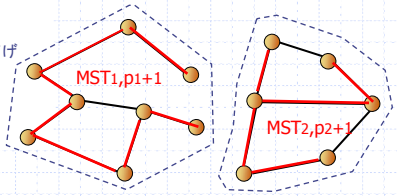
cost($\mathcal{T}$) ≦ 4Bの解$\mathcal{T}$を
見つけるか
opt(G,p) <Bと判定



w(e)>Bなる枝eを除去し
各連結成分GiでMSTiを求める
最適解の枝重み和 < 2 w(MSTi)

台数pの各成分への配分
pi := w(MSTi)/ 2B の切り下げ
(opt ≧Bなら pi+1 ≦ki)

各MSTiを 重み 4 B以下の
pi+1個の部分木に分解



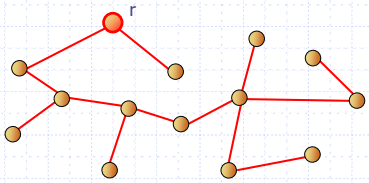
Ⅱ. Minmax Rooted Subtree Cover Problem (MRSC)

MRSC に対する3倍近似アルゴリズム

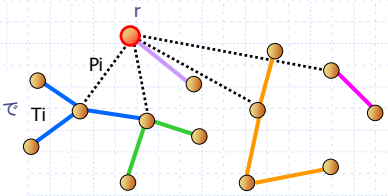
[Nagamochi 04]

GのMSTを求め
これを(2-2/(p+1))-近似の
p個の部分木Tiに分ける

各Tiに対し，rから最短路
Piを追加する．



Gかmetricのとき
根をデポとするp個のツアーで
Vをカバーする
minmax最適なものの
(6-4/(p+1))-近似解を作れる
（タイトな例あり）



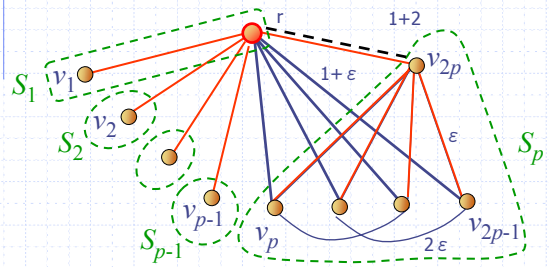
3倍近似アルゴリズムに対するタイトな例

[Nagamochi 04]

G: metric 完全グラフ （残りの枝重みは各１），ε =2/p

w(MST)=p+2

LB=max{(p+2)/p, 1+ ε }=1+2/p



木のMRSC に対する2倍近似アルゴリズム

[Nagamochi, Okada 03]

入力: 木 T=(V,E)，枝重み w(e)，根 r,
仮定 S={葉}, h(u)=0 for u ∈ S

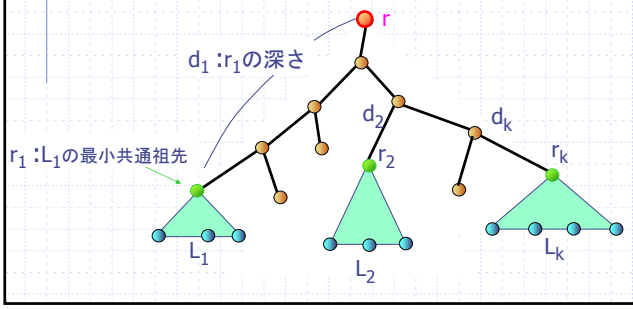
逆問題: 実数 x ≧0,
p(x;T) ≡ min p s.t. ∃$\mathcal{S}$ ={S1, S2, …, Sp} of V
cost($\mathcal{S}$) ≦ x

定理: Vの分割 $\mathcal{S}$ ={S1, S2, …, Sq} で
q ≦ p(x;T) かつ cost($\mathcal{S}$) ≦ 2x
なるものがO(n) 時間で求まる．

⇒ 2分探索 x ∈[LB,UB] (UB<3LB)
⇒ (2+ ε)-倍近似 in O(n $\log\log_{(1+\varepsilon/2)}3$) 時間

p(x;T) に対する下界

葉の部分集合の族 {L_1, L_2,…,L_k} が 独立 とは：
任意の T[L_i+r_i] と T[L_j+r] が枝素

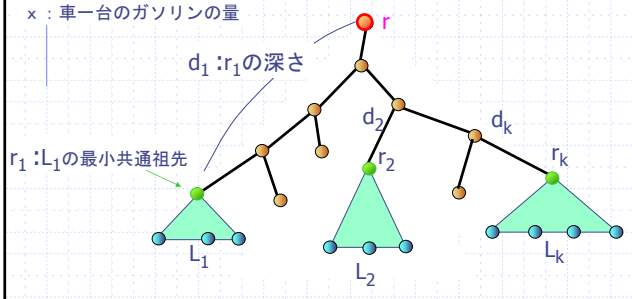


p(x;T) に対する下界

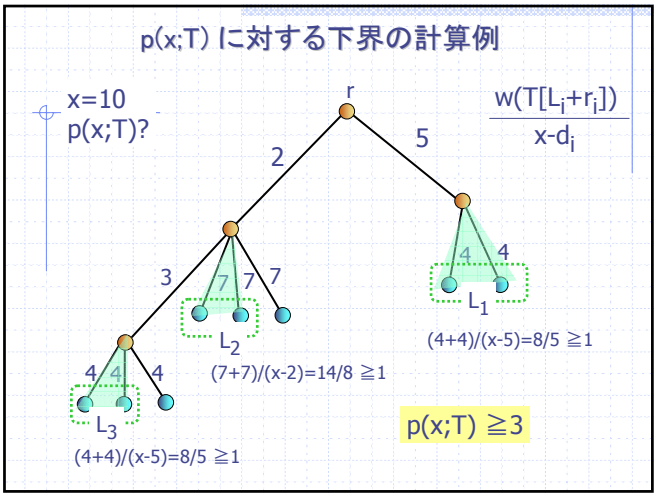
補題

$$\frac{w(T[L_1+r_1])}{x-d_1}+\frac{w(T[L_2+r_2])}{x-d_2}+\cdots+\frac{w(T[L_k+r_k])}{x-d_k}\leqq p(x;T)$$

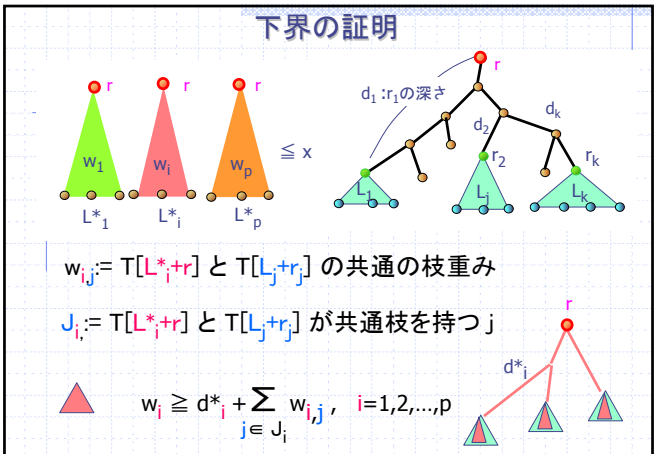
x ：車一台のガソリンの量



p(x;T) に対する下界の計算例



下界の証明

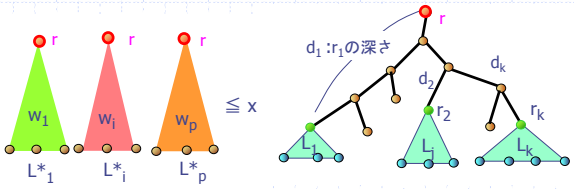


$w_{i,j}$:= T[L^*_i+r] と T[L_j+r_j] の共通の枝重み

J_i:= T[L^*_i+r] と T[L_j+r_j] が共通枝を持つ j

$$w_i \geqq d^*_i + \sum_{j \in J_i} w_{i,j}, \quad i=1,2,\ldots,p$$

下界の証明(続)

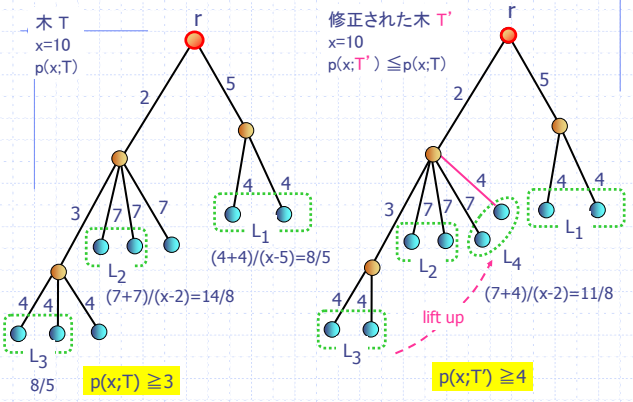


$$w_i \geqq d^*_i + \sum_{j \in J_i} w_{i,j}, \quad i=1,2,\ldots,p$$

$$w_i \geqq \frac{x\,(w_i - d^*_i)}{x - d^*_i} \geqq \frac{x}{x - d^*_i} \sum_{j \in J_i} w_{i,j} \geqq x \sum_{j \in J_i} \frac{w_{i,j}}{x - d_j}, \quad i=1,2,\ldots,p$$

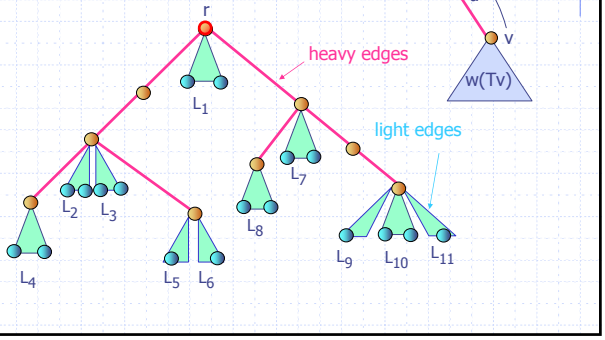
$$px \geqq \sum_{1 \leqq i \leqq p} w_i \geqq x \sum_{i} \sum_{j \in J_i} \frac{w_{i,j}}{x - d_j} = x \sum_{1 \leqq j \leqq k} \frac{\sum_{1 \leqq i \leqq p} w_{i,j}}{x - d_j} \geqq x \sum_{1 \leqq j \leqq k} \frac{w(T[L_j + r_j])}{x - d_j}$$

下界値の強化



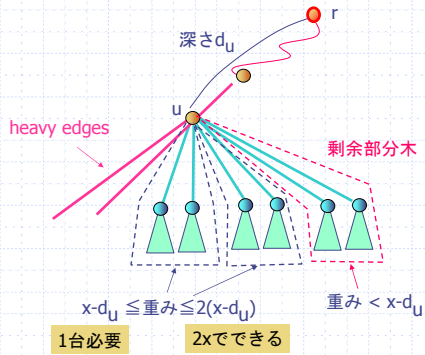
アルゴリズムの概略(1)

枝 (u,v) は heavy if $w(T_v)+d_v \geqq x$;
light otherwise.

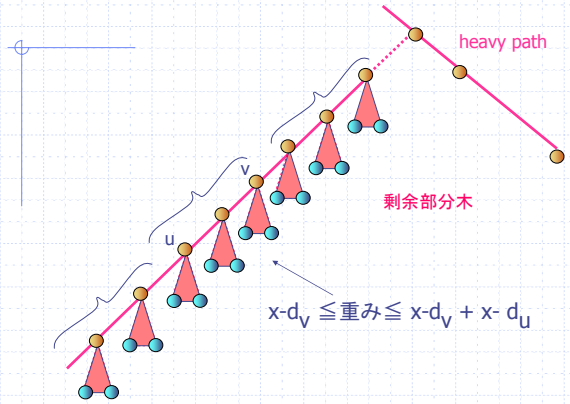


アルゴリズムの概略(2)

枝 (u,v) は heavy if $w(T_v)+d_v \geqq x$;
light if $w(T_v) < x-d_v$.



アルゴリズムの概略(3)



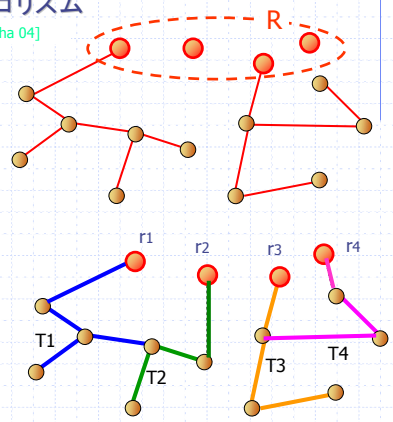
根の候補集合Rを持つMRSC に対する 4倍近似アルゴリズム

[Even, Garg, Konemann, Ravi, Sinha 04]

問題：各部分木はR内の点を根とする．他の部分木と同じ点を根としては共有しない．

Rを１点に縮約したグラフのMSTを求めるGでのMSTを作る各部分木を重み2B以下の部分木に分ける．

根の対していない部分木とRの残りの点との間で距離2B以下のマッチングをとる．



今後の課題

- 木に対する点素分割アルゴリズムの拡張
- 木に対する近似比2の改良
- 木，一般グラフに対して S⊂Vの場合の近似アルゴリズム
- metric，平面ユークリッド距離の場合のアルゴリズム
- 重みの総和，minmaxの二つの目的関数に対するトレードオフ
- 近似不可能度の調査
- 配送スケジューリング問題への適用
- メタヒューリスティックスとの組み合わせ

Workshop on
New Horizons in Computing

— Recent Trends in Theoretical Computer Science —

February 28 - March 3, 2005

Kyoto, Japan

Table of Contents

February 28 (Monday)

Fast and Sensitive Homology Search
Ming Li 340

Dynamic Graph Algorithms with Applications
Mikkel Thorup 341

Approximation Algorithms for Stochastic Combinatorial Optimization
R. Ravi 342

More Approximation Algorithms for Stochastic Programming Problems
David Shmoys 343

Efficient Haplotype Inference on Pedigrees and Applications in Gene Association Mapping
Tao Jiang 344

New Horizons in Machine Learning
Avrim Blum 345

Rigorous Analysis of Heuristics for NP-hard Problems
Uriel Feige 346

March 1 (Tuesday)

Data Stream Algorithms in Computational Geometry
Timothy M. Chan 356

Steps into Computational Algebraic Topology
Herbert Edelsbrunner 357

Efficient Algorithms for the Longest Path Problem
Ryuhei Uehara 358

Improved Approximation Algorithms for Metric Max TSP
Zhi-Zhong Chen 359

Proposal of Asynchronous Distributed Branch and Bound
Shigeru Masuyama 374

Energy-Optimal Online Algorithms for Broadcasting in Wireless Networks
Hirotaka Ono 375

Site-oriented Framework for Mining Communities on the Web
Yasuhiro Asano 377

On Right-Hand-on-the-Wall Traversal of Graphs
Kunihiko Sadakane 378
Distributing Distinct Integers Uniformly over a Square Matrix with Application to Digital Halftoning
Tetsuo Asano 379
Ultimate Implementation and Analysis of the AMO Algorithm for Pricing European-Asian Options
Akiyoshi Shioura 380

March 2 (Wednesday)

Algorithms for Modern Memory Systems
Martin Farach-Colton 381
Data Stream Algorithms and Applications
Shan Muthukrishnan 383
On Computing all Abductive Explanations from a Propositional Horn Theory
Kazuhisa Makino 384
How to Influence Noncooperative, Selfish Agents
Lisa K. Fleischer 385
Metric Labeling: Upper and Lower Bounds
Seffi Naor 386
Approximate Distance Oracles and Spanners with Sublinear Error Terms
Uri Zwick 387

March 3 (Thursday)

The Walkers Problem: On the Cycle and the Grid
Josep Diaz 388
Connectivity and Information Transfer in Social Networks
Richard Cole 391
Approximation Algorithms for Network Problems
Susanne Albers 392
Generalized linear programming
Jiří Matoušek 393
My Favorite Ten Complexity Theorems of the Past Decade II
Lance Fortnow 394
Some Heuristic Analysis of Average Behavior of Local Search Algorithms
Osamu Watanabe 395

Fast and Sensitive Homology Search

Ming Li*

School of Computer Science, University of Waterloo
(Canada Research Chair in Bioinformatics, Professor)
&
Computer Science Department, City University of Hong Kong
(Visiting Professor)

Homology search, finding similar parts between two sequences, is the most popular task in bioinformatics. A large fraction of the world's supercomputing time is consumed by homology search. We introduce the fundamental ideas and a mathematical theory of optimized spaced seeds. Based on such ideas, our software PatternHunter is significantly faster than current homology search tools such as BLAST, at higher sensitivity, or Smith-Waterman dynamic programming, at its full sensitivity. In just 3 years after their discovery, the optimal spaced seeds are directly benefiting thousands of researchers in the world, daily.

*Joint work with Bin Ma and John Tromp.

Dynamic graph algorithms with applications

Mikkel Thorup
AT&T

First we review amortized fully-dynamic polylogarithmic time algorithms for connectivity, MST, 2-edge- and biconnecitivity. Second we discuss how they yield improved static algorithms: connectivity in constructing a tree from homeomorphic subtrees and 2-edge connectivity for finding unique matchings in graphs.

Finally, on the more practical side, we will discuss how output senstive algorithms for dynamic shortest paths have been applied successfully in local search algorithms for improving routing on the internet, roughly doubling the capacity.

Approximation Algorithms for Stochastic Combinatorial Optimization

R. Ravi
Carnegie Mellon University

Two-stage stochastic programming with recourse is an attempt to model data uncertainty. Data for the current time (e.g. current costs, demands) are known, whereas the uncertain future is characterized by a given probability distribution. After a set of decisions are made in a first stage, the actual future is revealed (according to the probability distribution). The first-stage solution can then be augmented in a second recourse stage to obtain a feasible solution for the realized scenario. The goal is to minimize the sum of first-stage costs plus the expected costs in the second stage.

We consider several classical combinatorial optimization problems in this framework, and provide tight (up to small constants) approximation algorithms for them. In the talk, we will focus on a canonical problem in network design (Steiner trees). We consider different ways to model future uncertainty and present approximation algorithms based on boosted sampling and rounding an LP relaxation.

This talk describes recent work with Anupam Gupta, Martin Pal and Amitabh Sinha.

More approximation algorithms for stochastic programming problems

David B. Shmoys
Cornell University

Abstract

Stochastic optimization problems attempt to model uncertainty in the data by assuming that (part of) the input is specified in terms of a probability distribution, rather than by deterministic data given in advance; they have been studied since the 50's, and have become an important paradigm in a wide range of application areas, including transportation models, logistics, financial instruments, and network design. Particular attention has been paid to 2-stage models with recourse: first, given only distributional information about (some of) the data one commits on initial actions, and then once the actual data is realized (according to the distribution), further (recourse) actions can be taken. These problems pose significant computational obstacles, both from a practical perspective, as well as from the point of view of complexity theory.

There have been a number of recent results in that give approximation algorithms, that is, algorithms that are guaranteed to find solutions with provably near-optimal expected costs. However, these results are limited either in terms of the types of distributions that can be modeled, or in terms of the cost structure. We show that in a "black box" model for specifying the distribution, an arbitrary cost structure can be handled, and give the first constant-factor approximation algorithms for this setting. This is based on first designing a fully polynomial approximation scheme for solving the exponentially large (in *both* the constraints and variables) linear programming relaxation. We will discuss both these specific results, as well as to lay out a number of directions in which performance guarantees for stochastic programming problems might still be obtained.

This research is joint work with Chaitanya Swamy.

Efficient Haplotype Inference on Pedigrees and Applications in Gene Association Mapping

Jing Li * Tao Jiang †

Abstract

We discuss the problem of how to infer haplotypes from genotypes on pedigree data under the Mendelian law of inheritance and the minimum recombination principle. The problem is important for the construction of haplotype maps and genetic linkage/association analysis. We prove that the problem of finding a minimum-recombinant haplotype configuration is in general NP-hard. This is the first complexity result concerning the problem to our knowledge. An iterative algorithm based on blocks of consecutive resolved marker loci (called block-extension) is proposed. It is very efficient and can be used for large pedigrees with a large number of markers, especially for those data sets requiring few recombinants (or recombination events). A polynomial-time exact algorithm for haplotype reconstruction without recombinants is also presented. The algorithm first identifies all the necessary constraints based on the Mendelian law and the zero-recombinant assumption, and represents them as a system of linear equations over the cyclic group Z_2. By using a simple method based on Gaussian elimination, we could obtain all possible feasible haplotype configurations. Finally, we describe an integrated approach to haplotype inference and missing allele imputation based on integer linear programming (ILP). We have implemented the block-extension ILP algorithms and tested them on simulated data and real data. The results show that the programs perform very well on both types of data and will be useful for large scale haplotype inference projects. If time allows, we will also describe an application in gene association mapping.

*Department Electrical Engineering and Computer Science, Case Western Reserve University, Cleveland, Ohio. jingli@eecs.cwru.edu. Research supported by NSF grant CCR-9988353.

†Department of Computer Science, University of California - Riverside and Shanghai Center for Bioinformatics Technology. jiang@cs.ucr.edu. Research supported by NSF Grants CCR-0309902 and National Key Project for Basic Research (973) 2002CB512801.

New Horizons in Machine Learning

Avrim Blum*
Carnegie Mellon University

In this talk I will survey some of the current challenges and "hot topics" in the field of machine learning. I will then focus more specifically on one topic, kernel methods, that has become quite popular in machine learning, especially in conjunction with the notion of margins. Kernel functions allow one to implicitly map data into a high-dimensional space and perform certain operations there without paying a high price computationally. Furthermore, if the data has a large-margin separator in that space, then one can avoid paying a high price in terms of sample size as well. For example, this is the key idea underlying Support Vector Machines. I will discuss how techniques of random projection and dimensionality-reduction studied in the theory community can be used to provide insight into the behavior of kernels and what it is they really provide. In particular, I will show how given a kernel as a black-box function, we can use various forms of random projection to extract an explicit small feature space that captures much of the power of the given kernel.

*Portions of this talk are joint work with Nina Balcan and Santosh Vempala.

Rigorous Analysis of Heuristics for NP-hard Problems

Uriel Feige
Weizmann Institute, Israel
uriel.feige@weizmann.ac.il

Abstract

The known NP-hardness results imply that for many combinatorial optimization problems there are no efficient algorithms that find an optimal solution, or even a near optimal solution, on every instance. A heuristic for an NP-hard problem is a polynomial time algorithm that produces optimal or near optimal solutions on some input instances, but may fail on others. The study of heuristics involves both an algorithmic issue (the design of the heuristic algorithm) and a conceptual challenge, namely, how does one evaluate the quality of a heuristic. Current methods for evaluating heuristics include experimental evidence, hand waving arguments, and rigorous analysis of the performance of the heuristic on some wide (in a sense that depends on the context) classes of inputs. This talk is concerned with the latter method. On the conceptual side, several frameworks that have been used in order to model the classes of inputs of interest (including random models, semi-random models, smoothed analysis) will be discussed. On the algorithmic side, several algorithmic techniques and principles of analysis that are often useful in these frameworks will be presented.

1 Introduction

Given a computational problem, it is desirable to have algorithms that produce *optimal* results, are *efficient* (polynomial time), and work on *every* input instance. For many combinatorial problems, this goal is too ambitious, as shown by the theory of NP-completeness. Hence one should set goals that are more modest. Approaches that are tried and have firm theoretical foundations include approximation algorithms (relax the optimality

requirement) and fixed parameter tractability (refine the efficiency requirement). We shall discuss a different approach, that of *heuristics*, that relaxes the universality requirement. Here we define a heuristic to be a polynomial time algorithm that produces optimal results on *typical* inputs. The notion of a *typical* input is rather fuzzy, and a major conceptual challenge of the study of heuristics is to give this notion a rigorous meaning.

Some of the research goals of the study of heuristics are the following:

- Explain the apparent success of known heuristics.
- Come up with good heuristic ideas.
- Match heuristics to problems.
- Investigate fundamental limitations of the heuristic methodology.

If we wish to perform a mathematically rigorous study of heuristics, we may want to ask our selves how does one *prove* that a certain heuristic is good, and likewise, how does one *prove* that a certain heuristic is bad.

Here we use the following approach. One should first provide a rigorous definition of what the concept of *typical input* means. Given such a definition (for example, suppose that in some context, a typical graph can be assumed to be a planar graph), one is no longer dealing with the fuzzy notion of heuristics, but with the familiar notion of worst case analysis of algorithms. It will often be the case that we shall model a typical input as an input chosen at random from some well defined distribution. We remark that also in this case (of *average* case analysis), we will typically be performing worst case analysis. The reason for this is that usually analysis of algorithm in random models breaks down into two parts. One first establishes that random inputs are likely to have a certain property P (e.g., random graphs are likely to have very strong expansion properties), and then one shows an algorithm that work on every input that has property P.

2 Some theoretical frameworks

We sketch some theoretical frameworks that have been suggested in order to model typical inputs.

2.1 Random inputs

A good example is the $G_{n,p}$ model of random graphs.

An interesting algorithmic result [7] in this model is that there is a polynomial time algorithm that with high probability finds Hamiltonian a cycle in a random graph, even when p is so small such that the minimum degree in the graph is 2. (When the minimum degree is below 2, then certainly the graph does not have a Hamiltonian cycle.)

On the other hand, there are other NP-hard problems (such as max-clique) for which no polynomial time algorithm is known to produce optimal results on a random graph.

2.2 Planted solution models

When the random model seems too difficult, it may be useful to consider a *planted solution* model. For example, one can plant a clique of large size k in a random graph, and ask how large k can be so that a polynomial time algorithm can detect it. It is known that $k = \Omega(\sqrt{n})$ suffices [2].

2.3 Semi-random models, monotone adversaries

Given a specific random model (or planted solution model), there is danger that algorithms designed for the model will suffer from "over-fitting", and would not work under a slightly different model. To add robustness to algorithms, one may consider semi-random models, first suggested by Blum and Spencer [6].

Here is an example of what the author considers to be over-fitting. When $k \gg \sqrt{n \log n}$, the vertices of a planted k-clique almost surely are those of highest degree in an otherwise random graph. An algorithm may select the k highest degree vertices and check if they form a clique.

A specific version of semi-random models is that of the *monotone adversary* [10]. For example, in the planted clique model, the monotone adversary is allowed to remove arbitrarily many non-clique edges. The degree based algorithm no longer works. Still, more sophisticated algorithms based on semidefinite programming do work, up to $k = \Omega(\sqrt{n})$ [11].

2.4 Smoothed analysis

This model was advocated by Spielman and Teng [18]. The idea is to take an arbitrary input, but then to make a random perturbation to the input. This

may capture well situations where in a typical numerical input, the low order bits are random. Such a model was used in order to offer an explanation for the practical success of the simplex algorithm [18]. For NP-hard problems, it was shown that problems that have fully polynomial time approximation schemes are typically solved in polynomial time on smoothed instances [3].

2.5 Stable inputs

In some applications (such as clustering), the interesting inputs are those that are *stable* in the sense that a small perturbation in the input does not change the combinatorial solution. Bilu and Linial [5] define the notion of stable inputs, and present algorithms that solve NP-hard cut problems whenever the input instance is (highly) stable.

2.6 A comparison

In smoothed analysis, one first picks an arbitrary (worst case) instance. This instance defines a certain region in instance-space (all input instances that can be derived by small perturbations from the original instance). Then, a random input is chosen in this region.

In the monotone adversary model, first an instance is chosen at random, which then defines a region (all instances reachable from the original instance by monotone changes). Thereafter, an arbitrary (worst case) input is chosen in this region.

Hence in a sense, the difference between smoothed analysis and monotone adversary is mainly in the order of quantifiers (forall followed by random versus random followed by forall). In this respect, the monotone adversary model is more difficult.

For stable inputs, the regions in instance-space are determined by the combinatorial solution, rather than by the instance representation. A worst case region is picked, and within it, a worst case input, provided that it is far from the boundary of the region.

3 Algorithmic techniques

Common techniques for designing heuristics in some of the models presented above include detecting statistical irregularities induced by an optimal solution, the use of approximation algorithms, and "hill climbing" once a near optimal solution is found, using the fact that in many of these models near

optimal solutions are necessarily of small Hamming distance from the optimal solution.

3.1 Random 3SAT

We will use the well known problem of 3SAT to demonstrate some of the past rigorous work on analysis of heuristics. We shall consider a random 3CNF input formula f with n variables and m clauses, with $m \gg n$. The expected number of satisfying assignments for f is $(1-1/2^3)^m \cdot 2^n$, implying that when $m \gg n$ the formula is unlikely to be satisfiable.

We shall consider two tasks. One is to search for a satisfying assignment when the formula happens to be satisfiable. The other is to prove non-satisfiability for non-satisfiable formulas (refutation). We remark that for worst case analysis, refutation and search are strongly related (when a search procedure stops without finding a satisfying assignment, this serves as a refutation). For heuristics, we shall see that search and refutation may require very different algorithms.

3.2 Searching for a solution

There are algorithms that appear to very quickly find satisfying assignments in random formulas [8], and it would be very interesting to support this empirical finding by rigorous analysis. We are not able to do so at the moment. Here we present some results that can be proved rigorously.

When $m \gg n \log n$, then if the formula happens to be satisfiable, the satisfying assignment is likely to be unique. It then can be shown that the distribution on random satisfiable formulas can be approximated by the following distribution in the planted solution model.

Pick at random an assignment a to the variables. Choose clauses at random, discarding clauses not satisfied by a, until m clauses are reached. When $m \gg n \log n$, it is likely that a is the unique satisfying assignment.

The planted solution a induces some easily detectable statistical properties. For every variable x, in every clause C that contained x and was discarded, the polarity of x in C disagreed with its polarity in a. Set x according to the polarity that agrees with the majority of the occurrences of x in f. When $m \gg n \log n$, it is likely that this algorithm recovers a.

We now consider the more difficult case of $m = d \cdot n$ for some large constant d. In this case the distribution generated by the planted model is no longer known to be statistically close to that of random satisfiable

formulas. The reason is that the planted model favors formulas with many satisfying assignments. We shall present an algorithm that works in the planted model. It is not known whether this algorithm also extends to the model of random satisfiable formulas.

Given the formula f, start with an initial assignment $a(0)$ that is simply the majority vote assignment (breaking ties arbitrarily). A linear fraction of the variables (exponentially small in d) are likely to be set in disagreement with a, and a linear fraction of clauses are likely not to be satisfied by $a(0)$. We now move to a satisfying assignment by a "hill climbing" procedure. The procedure described here is taken from [13], and its analysis is based on [1, 14]. The procedure itself is a considerable simplification of the procedures described in [1, 14]. This simplification was achieved by following the methodology of considering semi-random inputs (a monotone adversary is allowed to add arbitrary clauses in which all three literals are set in agreement with a), which forces one to make algorithms more robust, and often helps clean away aspects of the algorithm that rely on too detailed statistical properties of the input distribution.

The hill climbing algorithm works it iterations. In each iteration, a local search is performed in order to improve the current assignment. Let $a(j)$ denote the assignment at iteration j, and let $T(j)$ be the set of clauses satisfied by $a(j)$.

Pick an arbitrary clause C not satisfied by $a(j)$. Find the assignment closest (in Hamming distance) to $a(j)$ that satisfies the sub-formula $T(j) \cup C$. Increment j and repeat.

The algorithm obviously finds a satisfying assignment. The only question is how fast.

To analyse the complexity of a single iteration, we let $h(j)$ denote the Hamming distance between $a(j)$ and $a(j+1)$. Since $a(j+1)$ can be reached from $a(j)$ by iteratively flipping variables in currently arbitrary unsatisfied clauses in $T(j) \cup C$, it follows that the time per iteration is at most $3 \cdot 2^{h-1} n^{O(1)}$, which is polynomial when $h = O(\log n)$.

The main technical lemma is that with high probability, in all iterations, $h < O(\log n)$. Hence the algorithm works in polynomial time. The proof of this lemma shows that with high probability, f has a *core* with properties as defined below, and that the algorithm works on *every* formula that has such a core.

A variable x for which $a(0) = a$ is a core variable if flipping it makes at least one clause in $T(0)$ not satisfied, and every assignment in which x is flipped that satisfies $T(0)$ requires flipping a linear number of other variables.

Probabilistic analysis shows that removing the core variables and simplifying the random formula f, it is likely to decompose into small sub-formulas of size $O(\log n)$, on disjoint sets of (non-core) variables.

In any formula (and initial assignment $a(0)$) that has such a core one has the following property. An iteration can be completed by $O(\log n)$ flips of non-core variables. Moreover, as long as $h = O(\log n)$, no core variable will accidently be flipped, and hence the above property is maintained in all iterations.

3.3 Refutation

If a formula is not satisfiable, the heuristic presented above takes exponential time to detect this. Hence we need a different heuristic for refutation.

A general approach for refutation may use approximation algorithms. When $m \gg n$, every assignment satisfies roughly $7m/n$ clauses of a random formula. An algorithm for approximating max-3SAT within a ratio better than 7/8 would refute most dense 3SAT formulas. Unfortunately, approximating max-3SAT (in the worst case) beyond 7/8 is NP-hard [16].

Turning the above algorithm around, we may ask what are the consequences of the hypothesis that there is no polynomial time algorithm for refuting dense random 3CNF formulas. This would imply that one cannot approximate max-3SAT within a ratio better than 7/8, which is a known (but very difficult) NP-hardness result. Many other hardness of approximation results would follow [9], some of which are currently not known to have NP-hardness analogues. The above hypothesis (regardless of its correctness) seems to be a good rule of thumb for conjecturing hardness of approximation results. Many of its predictions (with weaker constants) can be proved assuming that NP does not have sub-exponential algorithms [17].

So how does one refute random 3CNF formulas? When $m > n^2$ one can do the following. There are roughly $3n$ clauses containing the variable x_1. It suffices to refute the sub-formula f_1 containing these clauses. Substitute $x_1 = 0$ and simplify f_1 to a 2SAT formula. This is a random formula with roughly $3n/2$ clauses, and hence is unlikely to be satisfiable. 2SAT can be decided in polynomial time. Repeating the above argument with $x_1 = 1$ refutes f_1.

As m gets smaller, refutation gets harder. The best algorithms known for refuting random 3SAT [12] require $m > cn^{3/2}$ (where experimentation shows that one can take $c = 2.5$). These algorithms are based on pair-wise statistical irregularities and eigenvalue computations. This approach was

initiated in [15] for 4SAT. We sketch this approach.

Consider a random 4SAT formula f with $m \gg n^2$ clauses. In a satisfying assignment a, at least half the variables are negative. (A complimentary argument handles the case that at least half of the variables are positive in a.) Let S be the set of variables negative in a. observe that there cannot be a positive clause in f whose four variables are in S. Construct a graph G on $N = \binom{n}{2}$ vertices, in which every pair of variables is a vertex, and every positive clause $(x_i \vee x_j \vee x_k \vee x_l)$ contributes an edge $([x_i x_j], [x_k x_l])$. If f is satisfiable then S induces an independent set of size $N/4$. Hence to refute f it suffices to show that G has no independent set of size $N/4$. But when f is random, the graph G is random, and the condition $m \gg n^2$ implies that G has a large linear number of edges. Such graphs do not have large independent sets. Moreover, this can be certified efficiently by eigenvalue techniques (or by semidefinite programming, using the theta function of Lovasz).

In combination with some additional ideas, the above approach extends to refuting random 3SAT formulas with $m > cn^{3/2}$ clauses for large enough c [12]. It is not know how to refute random 3SAT formulas with less than $n^{3/2}$ clauses. In particular, it is known that when m is much smaller than $n^{3/2}$, resolution would take exponential time [4], and that certain semidefinite programming approaches (reducing 3SAT to independent set on a graph with $7m$ vertices, and computing the theta function of the resulting graph) would not work.

4 Summary

We presented some rigorous models in which one can study heuristics. We presented some algorithmic results in these models (the presentation was biased towards algorithms that the author is more familiar with). There are also hardness results for some of these models, showing that under certain settings of the parameters of the model, no heuristic will work. This is beyond the scope of this presentation, but see [10] for example.

Two points that we wish to make is that in principle, it is possible to study heuristics in a mathematically rigorous way, and that once this is done, the design of heuristics may require quite sophisticated algorithmic ideas and supporting mathematical analysis. But perhaps the main point is that the rigorous study of heuristics is still a young and wide open research area.

Acknowledgements

This research of the author is partly supported by a grant from the German Israeli Foundation (GIF). This manuscript was prepared when the author was visiting Microsoft Research at Redmond, Washington.

References

[1] Noga Alon, Nabil Kahale: A Spectral Technique for Coloring Random 3-Colorable Graphs. SIAM J. Comput. 26(6): 1733-1748 (1997).

[2] Noga Alon, Michael Krivelevich, Benny Sudakov: Finding a Large Hidden Clique in a Random Graph. SODA 1998: 594-598.

[3] Rene Beier, Berthold Voecking: Typical properties of winners and losers in discrete optimization. STOC 2004: 343-352.

[4] Eli Ben-Sasson, Avi Wigderson: Short proofs are narrow - resolution made simple. J. ACM 48(2): 149-169 (2001).

[5] Yonatan Bilu, Nati Linial: Are stable instances easy? Manuscript (2004).

[6] Avrim Blum, Joel Spencer: Coloring Random and Semi-Random k-Colorable Graphs. J. Algorithms 19(2): 204-234 (1995).

[7] Bela Bollobas, Trevor I. Fenner, Alan M. Frieze: An algorithm for finding Hamilton cycles in a random graph. Combinatorica 7(4): 327-341 (1987).

[8] A. Braunstein, M. Mezard, R. Zecchina: Survey propagation: an algorithm for satisfiability. Manuscript (2002).

[9] Uriel Feige: Relations between average case complexity and approximation complexity. STOC 2002: 534-543.

[10] Uriel Feige, Joe Kilian: Heuristics for Semirandom Graph Problems. J. Comput. Syst. Sci. 63(4): 639-671 (2001).

[11] Uriel Feige, Robert Krauthgamer: Finding and certifying a large hidden clique in a semirandom graph. Random Struct. Algorithms 16(2): 195-208 (2000).

[12] Uriel Feige, Eran Ofek: Easily Refutable Subformulas of Large Random 3CNF Formulas. ICALP 2004: 519-530.

[13] Uriel Feige, Dan Vilenchik: A Local Search Algorithm for 3SAT. Technical Report MCS 04-07, Computer Science and Applied Mathematics, The Weizmann Institute of Science (2004).

[14] Abraham Flaxman: A spectral technique for random satisfiable 3CNF formulas. SODA 2003: 357-363.

[15] Andreas Goerdt, Michael Krivelevich: Efficient Recognition of Random Unsatisfiable k-SAT Instances by Spectral Methods. STACS 2001: 294-304.

[16] Johan Hastad: Some optimal inapproximability results. J. ACM 48(4): 798-859 (2001).

[17] Subhash Khot: Ruling Out PTAS for Graph Min-Bisection, Densest Subgraph and Bipartite Clique. FOCS 2004: 136-145.

[18] Daniel A. Spielman, Shang-Hua Teng: Smoothed analysis of algorithms: why the simplex algorithm usually takes polynomial time. STOC 2001: 296-305.

Data Stream Algorithms in Computational Geometry

Timothy M. Chan*
University of Waterloo

The data stream model has received considerable attention in recent years, due to its ability to cope with massive data sets. The model is simple: an algorithm makes one (or a small number of) pass(es) over the input and is allowed to store only a limited amount of information at any moment in time.

In this talk, we discuss some recent results about streaming algorithms in computational geometry. A number of basic geometric problems are considered, and a few different types of streaming algorithms are explored. For example:

- we describe a one-pass algorithm that can compute approximate extents (or convex hulls) in fixed dimensions, using only a constant amount of space;
- we describe a sliding-window algorithm to maintain an approximation to the diameter of a low-dimensional point set, using $O(\log R)$ space, where R is a bound on the distance ratio;
- we show that if a constant number of passes is allowed, then certain geometric problems, such as low-dimensional linear programming, can actually be solved exactly, using $O(n^\delta)$ space, for any fixed $\delta > 0$.

*Some parts of the talk are joint work with B. Sadjad and with E. Y. Chen.

Steps into Computational Algebraic Topology

Herbert Edelsbrunner
Arts and Sciences Professor of Computer Science and Mathematics
Duke University

A nested sequence of progressively larger topological spaces implies a sequence of homology groups connected by maps induced by the inclusions of the corresponding spaces. For each pair of groups, we call the image of the earlier in the later group a *persistent homology group*. Given a function on a topological space, the sublevel sets form such a nested sequence of spaces. The corresponding persistent homology groups can be encoded using a finite multiset in the extended plane. We call this multiset the *persistence diagram* of the function. Assuming a triangulation of the space and a piecewise linear function, we have an algorithm that computes the persistence diagram in worst-case time cubic in the size of the triangulation. However, its observed running time is vastly better so that even triangulations with a few million simplices can be processed in a matter of seconds. We have proved that for two continuous functions on a common space, the Fréchet bottleneck distance between the two diagrams is bounded from above by the maximum norm of the difference function.

We justify the introduction of the above concepts and the design and implementation of their algorithms by three applications:

(i) the estimation of the homology of a shape from a finite point sample;

(ii) the establishment of a new bound on the difference between the total mean curvatures of two topologically equivalent surfaces;

(iii) the development of a coarse docking algorithm for proteins based on the detection of shape features on a continuum of scale levels.

Efficient Algorithms for the Longest Path Problem

Ryuhei Uehara
JAIST

The longest path problem is to find a longest path in a given graph. While the graph classes in which the Hamiltonian path problem can be solved efficiently are widely investigated, few graph classes are known to be solved efficiently for the longest path problem. We show some efficient algorithms for the longest path problems for some graph classes. The complexity of the longest path problem for interval graphs, convex graphs, and biconvex graphs is remained open.

Improved Approximation Algorithms for Metric Max TSP

Zhi-Zhong Chen * Takayuki Nagoya †

Abstract

We present two $O(n^3)$-time approximation algorithms for the metric case of the maximum traveling salesman problem, where n is the number of vertices in the input (undirected or directed) graph. One of them is for directed graphs and its approximation ratio is $\frac{27}{35}$. The other is for undirected graphs and its approximation ratio is $\frac{7}{8} - o(1)$. Both algorithms improve on the previous bests.

1 Introduction

The *maximum traveling salesman problem* (MaxTSP) is to compute a maximum-weight Hamiltonian circuit (called a *tour*) in a given complete edge-weighted (undirected or directed) graph. Usually, MaxTSP is divided into the *symmetric* and the *asymmetric* cases. In the symmetric case, the input graph is undirected; we denote this case by SymMaxTSP. In the asymmetric case, the input graph is directed; we denote this case by AsymMaxTSP. Note that SymMaxTSP can be trivially reduced to AsymMaxTSP.

A natural constraint one can put on AsymMaxTSP and SymMaxTSP is the *triangle inequality* which requires that for every set of three vertices u_1, u_2, and u_3 in the input graph G, $w(u_1, u_2) \leq w(u_1, u_3) + w(u_3, u_2)$, where $w(u_i, u_j)$ is the weight of the edge from u_i to u_j in G. If we put this constraint on AsymMaxTSP, we obtain a problem called *metric* AsymMaxTSP. Similary, if we put this constraint on SymMaxTSP, we obtain a problem called *metric* SymMaxTSP.

Both metric SymMaxTSP and metric AsymMaxTSP are Max-SNP-hard [1] and there have been a number of approximation algorithms known for them [7, 4, 5]. In 1985, Kostochka and Serdyukov [7] gave an $O(n^3)$-time approximation algorithm for metric SymMaxTSP that achieves an approximation ratio of $\frac{5}{6}$. Their algorithm is very simple and elegant. Tempted by improving the ratio $\frac{5}{6}$, Hassin and Rubinstein [4] gave a randomized $O(n^3)$-time approximation algorithm for metric SymMaxTSP whose *expected* approximation ratio is $\frac{7}{8} - o(1)$. This randomized algorithm was recently (partially) derandomized by Chen *et al.* [3]; their result is a (deterministic) $O(n^3)$-time approximation algorithm for metric SymMaxTSP whose approximation ratio is $\frac{17}{20} - o(1)$. In this paper, we completely derandomize the randomized algorithm, i.e., we obtain a (deterministic) $O(n^3)$-time approximation algorithm for metric SymMaxTSP whose approximation ratio is $\frac{7}{8} - o(1)$. Our algorithm also has the advantage of being easy to parallelize. Our derandomization is based

*Supported in part by the Grant-in-Aid for Scientific Research of the Ministry of Education, Science, Sports and Culture of Japan, under Grant No. 14580390. Department of Mathematical Sciences, Tokyo Denki University, Hatoyama, Saitama 350-0394, Japan. Email: chen@r.dendai.ac.jp.

†Department of Mathematical Sciences, Tokyo Denki University, Hatoyama, Saitama 350-0394, Japan. Email: nagoya@r.dendai.ac.jp.

on the idea of Chen *et al.* [3] and newly discovered properties of a folklore partition of the edges of a $2n$-vertex complete undirected graph into $2n-1$ perfect matchings. These properties may be useful elsewhere. In particular, one of the properties says that if $G = (V, E)$ is a $2n$-vertex complete undirected graph and M is a perfect matching of G, then we can partition $E - M$ into $2n-2$ perfect matchings $M_1, \ldots, M_{2n-2}$ among which there are at most $k^2 - k$ perfect matchings M_i such that the graph $(V, M \cup M_i)$ has a cycle of length at most $2k$ for every natural number k. This property is interesting because Hassin and Rubinstein [4] prove that if G and M are as before and M' is a random perfect matching of G, then with probability $1 - o(1)$ the multigraph $(V, M \cup M')$ has no cycle of length at most $\sqrt{n}$. Our result shows that instead of sampling from the set of all perfect matchings of G, it suffices to sample from $M_1, \ldots, M_{2n-2}$. This enables us to completely derandomize their algorithm.

As for metric AsymMaxTSP, Kostochka and Serdyukov [7] gave an $O(n^3)$-time approximation algorithm that achieves an approximation ratio of $\frac{3}{4}$. Their result remained the best in two decades until Kaplan *et al.* [5] gave a polynomial-time approximation algorithm whose approximation ratio is $\frac{10}{13}$. The key in their algorithm is a polynomial-time algorithm for computing two cycle covers $\mathcal{C}_1$ and $\mathcal{C}_2$ in the input graph G such that $\mathcal{C}_1$ and $\mathcal{C}_2$ do not share a 2-cycle and the sum of their weights is at least twice the optimal weight of a tour of G. They then observe that the multigraph formed by the edges in 2-cycles in $\mathcal{C}_1$ and $\mathcal{C}_2$ can be split into two subtours of G. In this paper, we show that the multigraph formed by the edges in 2-cycles in $\mathcal{C}_1$ and $\mathcal{C}_2$ *together with* a constant fraction of the edges in non-2-cycles in $\mathcal{C}_1$ and $\mathcal{C}_2$ can be split into two subtours of G. This enables us to improve Kaplan *et al.*'s algorithm to a polynomial-time approximation algorithm whose approximation ratio is $\frac{27}{35}$.

2 Basic Definitions

Throughout this paper, a *graph* means a simple undirected or directed graph (i.e., it has neither multiple edges nor self-loops), while a multigraph may have multiple edges but no self-loops.

Let G be a multigraph. We denote the vertex set of G by $V(G)$, and denote the edge set of G by $E(G)$. For a subset F of $E(G)$, $G - F$ denotes the graph obtained from G by deleting the edges in F. Two edges of G are *adjacent* if they share an endpoint.

Suppose G is undirected. The *degree* of a vertex v in G is the number of edges incident to v in G. A *cycle* in G is a connected subgraph of G in which each vertex is of degree 2. A *cycle cover* of G is a subgraph H of G with $V(H) = V(G)$ in which each vertex is of degree 2. A *matching* of G is a (possibly empty) set of pairwise nonadjacent edges of G. A *perfect matching* of G is a matching M of G such that each vertex of G is an endpoint of an edge in M.

Suppose G is directed. The *indegree* of a vertex v in G is the number of edges entering v in G, and the *outdegree* of v in G is the number of edges leaving v in G. A *cycle* in G is a connected subgraph of G in which each vertex has indegree 1 and outdegree 1. A *cycle cover* of G is a subgraph H of G with $V(H) = V(G)$ in which each vertex has indegree 1 and outdegree 1. A *2-path-coloring* of G is a partition of $E(G)$ into two subsets E_1 and E_2 such that both graphs $(V(G), E_1)$ and $(V(G), E_2)$ are collections of vertex-disjoint paths. G is *2-path-colorable* if it has a 2-path-coloring.

Suppose G is undirected or directed. A *path* in G is either a single vertex of G or a subgraph of G that can be transformed to a cycle by adding a single (new) edge. The *length* of a cycle or path C is the number of edges in C. A *k-cycle* is a cycle of length k. A *3^+-cycle* is a cycle of length

at least 3. A *tour* (also called a *Hamiltonian cycle*) of G is a cycle C of G with $V(C) = V(G)$. A *subtour* of G is a subgraph H of G which is a collection of vertex-disjoint paths.

A *closed chain* is a directed graph that can be obtained from an undirected k-cycle C with $k \geq 3$ by replacing each edge $\{u, v\}$ of C with the two directed edges (u, v) and (v, u). Similarly, an *open chain* is a directed graph that can be obtained from an undirected path P by replacing each edge $\{u, v\}$ of P with the two directed edges (u, v) and (v, u). An open chain is *trivial* if it is a single vertex. A *chain* is a closed or open chain. A *partial chain* is a subgraph of a chain.

For a graph G and a weighting function w mapping each edge e of G to a nonnegative real number $w(e)$, the *weight* of a subset F of $E(G)$ is $w(F) = \sum_{e \in F} w(e)$, and the *weight* of a subgraph H of G is $w(H) = w(E(H))$.

3 New Algorithm for Metric AsymMaxTSP

Throughout this section, fix an instance (G, w) of metric AsymMaxTSP, where G is a complete directed graph and w is a function mapping each edge e of G to a nonnegative real number $w(e)$. For each cycle C in G, we define its *reversal* to be the cycle obtained by reversing the direction of each edge in C. Note that C is the reversal of its reversal. Moreover, C is its reversal if and only if C is a 2-cycle.

Let OPT be the weight of a maximum-weight tour in G. Our goal is to compute a tour in G whose weight is large compared to OPT. We first review Kaplan *et al.*'s algorithm and define several notations on the way.

3.1 Kaplan et al.'s Algorithm

The key in their algorithm is the following:

Theorem 3.1 [5] *We can compute two cycle covers $\mathcal{C}_1$, $\mathcal{C}_2$ in G in polynomial time that satisfy the following two conditions:*

1. *$\mathcal{C}_1$ and $\mathcal{C}_2$ do not share a 2-cycle. In other words, if C is a 2-cycle in $\mathcal{C}_1$ (respectively, $\mathcal{C}_2$), then $\mathcal{C}_2$ (respectively, $\mathcal{C}_1$) does not contain at least one edge of C.*
2. *$w(\mathcal{C}_1) + w(\mathcal{C}_2) \geq 2 \cdot OPT$.*

Let G_2 be the subgraph of G such that $V(G_2) = V(G)$ and $E(G_2)$ consists of all edges in 2-cycles in $\mathcal{C}_1$ and/or $\mathcal{C}_2$. Then, G_2 is a collection of vertex-disjoint chains. For each closed chain C in G_2, we can compute two edge-disjoint tours T_1 and T_2 (each of which is of length at least 3), modify $\mathcal{C}_1$ by substituting T_1 for the 2-cycles shared by C and $\mathcal{C}_1$, modify $\mathcal{C}_2$ by substituting T_2 for the 2-cycles shared by C and $\mathcal{C}_2$, and further delete C from G_2. After this modification of $\mathcal{C}_1$ and $\mathcal{C}_2$, the two conditions in Theorem 3.1 still hold. So, we can assume that there is no closed chain in G_2.

For each $i \in \{1, 2\}$, let $W_{i,2}$ denote the total weight of 2-cycles in $\mathcal{C}_i$, and let $W_{i,3} = w(\mathcal{C}_i) - W_{i,2}$. For convenience, let $W_2 = \frac{1}{2}(W_{1,2} + W_{2,2})$ and $W_3 = \frac{1}{2}(W_{1,3} + W_{2,3})$. Then, by Condition 2 in Theorem 3.1, we have $W_2 + W_3 \geq OPT$. Moreover, using an idea in [7], Kaplan *et al.* observed the following:

Lemma 3.2 [5] *We can use $\mathcal{C}_1$ and $\mathcal{C}_2$ to compute a tour T of G with $w(T) \geq \frac{3}{4}W_2 + \frac{5}{6}W_3$ in polynomial time.*

Since each nontrivial open chain has a 2-path-coloring, we can use G_2 to compute a tour T' of G with $w(T') \geq W_2$ in polynomial time. Combining this observation, Lemma 3.2, and the fact that $W_2 + W_3 \geq OPT$, the heavier one between T and T' is of weight at least $\frac{10}{13}OPT$.

3.2 Details of the New Algorithm

The idea behind our new algorithm is to improve the second tour T' in Kaplan *et al.*'s algorithm so that it has weight at least $W_2 + \frac{1}{9}W_3$. The tactics is to add some edges of 3^+-cycles in $\mathcal{C}_i$ with $W_{i,3} = \max\{W_{1,3}, W_{2,3}\}$ to G_2 so that G_2 remains 2-path-colorable. Without loss of generality, we may assume that $W_{1,3} \geq W_{2,3}$. Then, our goal is to add some edges of 3^+-cycles in $\mathcal{C}_1$ to G_2 so that G_2 remains 2-path-colorable.

We say that an open chain P in G_2 *spoils* an edge (u, v) of a 3^+-cycle in $\mathcal{C}_1$ if u and v are the two endpoints of P. Obviously, adding a spoiled edge to G_2 destroys the 2-path-colorability of G_2. Fortunately, there is no 3^+-cycle in $\mathcal{C}_1$ in which two consecutive edges are both spoiled. So, let C_1, $\ldots$, C_ℓ be the 3^+-cycles in $\mathcal{C}_1$; we modify each C_j $(1 \leq j \leq \ell)$ as follows (see Figure 1):

- For every two consecutive edges (u, v) and (v, x) of C_j such that (u, v) is spoiled, replace (u, v) by the two edges (u, x) and (x, v). (*Comment*: We call (u, x) a *bypass edge* of C_j, call the 2-cycle between v and x a *dangling 2-cycle* of C_j, and call v the *articulation vertex* of the dangling 2-cycle. We also say that the bypass edge (u, x) and the dangling 2-cycle between v and x *correspond* to each other.)

We call the above modification of C_j the *bypass operation* on C_j. Note that applying the bypass operation on C_j does not decrease the weight of C_j because of the triangle inequality. Moreover, the edges of C_j not contained in dangling 2-cycles of C_j form a cycle. We call it the *primary cycle* of C_j. Note that C_j may have neither bypass edges nor dangling 2-cycles (this happens when C_j has no bad edges).

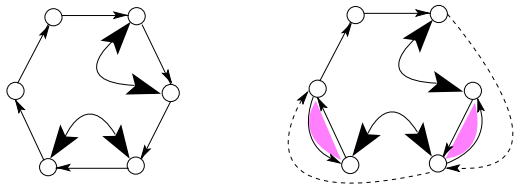


Figure 1: (1) A 3^+-cycle C_j (formed by the one-way edges) in $\mathcal{C}_1$ and the open chains (each shown by a two-way edge) each of which has a parallel edge in C_j. (2) The modified C_j (formed by the one-way edges), where bypass edges are dashed and dangling 2-cycles are painted.

Let H be the union of the modified C_1, $\ldots$, C_ℓ, i.e., let H be the directed graph with $V(H) = \bigcup_{1 \leq j \leq \ell} V(C_j)$ and $E(H) = \bigcup_{1 \leq j \leq \ell} E(C_j)$. We next show that $E(H)$ can be partitioned into three subsets each of which can be added to G_2 without destroying its 2-path-colorability. Before proceeding to the details of the partitioning, we need several definitions and lemmas.

Two edges (u_1, u_2) and (v_1, v_2) of H form a *critical pair* if u_1 and v_2 are the endpoints of some open chain in G_2 and u_2 and v_1 are the endpoints of another open chain in G_2 (see Figure 2). Note that adding both (u_1, v_1) and (u_2, v_2) to G_2 destroys its 2-path-colorability. An edge of H is *critical* if it together with another edge of H forms a critical pair. Note that for each critical edge e of H, there is a unique edge e' in H such that e and e' form a critical pair. We call e' the *rival* of e. An edge of H is *safe* if it is not critical. A *bypass edge* of H is a bypass edge of a C_j with $1 \leq j \leq \ell$. Similarly, a *dangling 2-cycle* of H is a dangling 2-cycle of a C_j with $1 \leq j \leq \ell$. A *dangling edge* of H is an edge in a dangling 2-cycle of H.

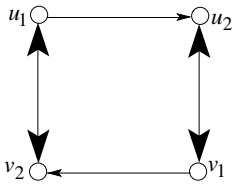


Figure 2: A critical pair formed by edges (u_1, u_2) and (v_1, v_2).

Lemma 3.3 *No bypass edge of H is critical.*

PROOF. Suppose that $e = (u_1, u_2)$ is a bypass edge of a C_j with $1 \leq j \leq \ell$. Then, u_2 is the articulation vertex of a dangling 2-cycle C of C_j. Let u_3 be the vertex of C other than u_2. Then, there is an open chain P in G_2 whose endpoints are u_1 and u_3. Since e leaves u_1 and $e' = (u_2, u_3)$ is the unique edge entering u_3, e' has to be the rival of e whenever e is critical. However, by the definition of criticalness, each critical edge and its rival should not be adjacent. So, e cannot be critical. □

Lemma 3.4 *Fix a j with $1 \leq j \leq \ell$. Suppose that an edge e of C_j is a critical dangling edge of H. Let C be the dangling 2-cycle of C_j containing e. Let e' be the rival of e. Then, the following statements hold:*

1. *e' is also an edge of C_j.*
2. *If e' is also a dangling edge of H, then the primary cycle of C_j consists of the two bypass edges corresponding to C and C', where C' is the dangling 2-cycle of C_j containing e'.*
3. *If e' is not a dangling edge of H, then e' is the edge in the primary cycle of C_j whose head is the tail of the bypass edge corresponding to C.*

PROOF. Let u_1 be the articulation vertex of C, and let u_2 be the other vertex of C. Then, there is an open chain P one of whose endpoints is u_2. Let u_3 be the other endpoint of P. We now prove the statemetns separately as follows.

Statement 1. Note that u_3 must be a vertex of C_j (indeed, (u_3, u_1) is a bypass edge of C_j). By the definition of criticalness, the rival of e is an edge incident to u_3. However, every edge of H incident to u_3 is in C_j. Thus, the rival of e must be in C_j whenever e is critical.

Statement 2. Suppose that e' is also a dangling edge of H. Then, since e' is incident to u_3 (as observed in the proof of Statement 1) and u_3 appears in the primary cycle of C_j, u_3 must be the

articulation vertex of the dangling 2-cycle C' containing e'. Let u_4 be the vertex of C' other than u_3. Then, by the definition of criticalness, there is an open chain in G_2 whose endpoints are u_4 and u_1. Now, (u_1, u_3) has to be the bypass edge corresponding to C'. Recall that (u_3, u_1) is the bypass edge corresponding to C. This completes the proof of Statement 2.

Statement 3. Suppose that e' is not a dangling edge of H. Recall that e' is incident to u_3 and (u_3, u_1) is a bypass edge of C_j. By Lemma 3.3, e' cannot be (u_3, u_1). So, e' has to be the edge in the primary cycle of C_j entering u_3. □

Lemma 3.5 *Fix a j with $1 \leq j \leq \ell$ such that the primary cycle C of C_j contains no bypass edge. Let $u_1, \ldots, u_k$ be a cyclic ordering of the vertices in C. Then, the following hold:*

1. *Suppose that there is a chain P in G_2 whose endpoints appear in C but not consecutively (i.e., its endpoints are not connected by an edge of C). Then, at least one edge of C is safe.*
2. *Suppose that every edge of C is critical. Then, there is a unique $C_{j'}$ with $j' \in \{1, \ldots, \ell\} - \{j\}$ such that (1) the primary cycle C' of $C_{j'}$ has exactly k vertices and (2) the vertices of C' have a cyclic ordering $v_1, \ldots, v_k$ such that for every $1 \leq i \leq k$, u_i and v_{k-i+1} are the endpoints of some chain in G_2.* (See Figure 4.)

Proof. We prove the two statements separately as follows.

Statement 1. By the existence of P, we can find two vertices u_i and u_h in C with $i < h$ such that (1) neither (u_i, u_h) nor (u_h, u_i) is an edge of C, (2) there is a chain in G_2 whose endpoints are u_i and u_h, and (3) there is no chain in G_2 whose endpoints both are in the set $\{u_{i+1}, u_{i+2}, \ldots, u_{h-1}\}$. Obviously, (u_i, u_{i+1}) is safe.

Statement 2. Each vertex u_i of C is an endpoint of a chain P_i in G_2 or else the two edges incident to u_i would be safe. Moreover, $P_1 \neq P_2$, $P_2 \neq P_3$, $\ldots$, $P_{k-1} \neq P_k$, and $P_k \neq P_1$ because we have applied the bypass operation on C_j. Furthermore, by Statement 1, there do not exist i and h with $1 \leq i \neq h \leq k$ with $P_i = P_h$. Therefore, for every $i \in \{1, \ldots, k\}$, the endpoint of P_i other than u_i is not in C.

For each $i \in \{1, \ldots, k\}$, let v_{k-i+1} be the endpoint of P_i other than u_i. Obviously, for each $i \in \{1, \ldots, k-1\}$, (v_{k-i}, v_{k-i+1}) has to be an edge of H because (u_i, u_{i+1}) is a critical edge. Similarly, (v_k, v_1) has to be an edge of H because (u_k, u_1) is a critical edge. So, $v_1, \ldots, v_k$ is a cyclic ordering of the vertices of some cycle C' in H. Let j' be the integer in $\{1, \ldots, \ell\}$ such that C' is a cycle in $C_{j'}$.

It remains to show that C' is not a dangling 2-cycle of $C_{j'}$. For a contradiction, assume that C' is a dangling 2-cycle of $C_{j'}$. Then, by Statement 1 in Lemma 3.4, $j = j'$ and C has to be the primary cycle of $C_{j'}$. Moreover, since C' is a 2-cycle, C is a 2-cycle, too. But then, $\{u_1, u_2\} \cap \{v_1, v_2\} \neq \emptyset$, because the articulation vertex of C' has to be a vertex of C. This contradicts the fact that for each $i \in \{1, \ldots, k\}$, the endpoint of P_i other than u_i is not in C (as observed above). □

Now we are ready to describe how to partition $E(H)$ into three subsets each of which can be added to G_2 without destroying its 2-path-colorability. We use the three colors 0, 1, and 2 to represent the three subsets, and want to assign each edge of $E(H)$ a color in $\{0, 1, 2\}$ so that the following conditions are satisfied:

(C1) For every critical edge e of H, e and its rival receive different colors.

(C2) For every dangling 2-cycle C of H, the two edges in C receive the same color.

(C3) If two adjacent edges of H receive the same color, then they form a 2-cycle of H.

To compute a coloring of the edges of H satisfying the above three conditions, we process C_1, ..., C_ℓ in an arbitrary order. While processing C_j ($1 \leq j \leq \ell$), we color the edges of C_j by distinguishing four cases as follows (where C denotes the primary cycle of C_j):

Case 1: C is a 2-cycle. Then, C contains either one or two bypass edges. In the former (respectively, latter) case, we color the edges of C_j as shown in Figure 3(2) (respectively, Figure 3(1)). Note that the colored edges satisfy Conditions (C1) through (C3) above.

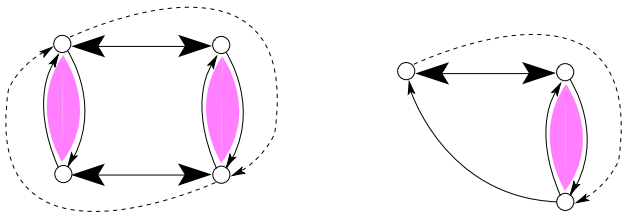


Figure 3: Coloring C_j when its primary cycle is a 2-cycle.

Case 2: Every edge of C is critical. Then, by Lemma 3.3, C contains no bypass edge. Let j' be the integer in $\{1, \ldots, \ell\} - \{j\}$ such that $C_{j'}$ satisfies the two conditions (1) and (2) in Statement 2 in Lemma 3.5. Then, by Lemma 3.4 and Statement 2 in Lemma 3.5, neither C_j nor $C_{j'}$ has a bypass edge or a dangling 2-cycle. So, the primary cycle of C_j (respectively, $C_{j'}$) is C_j (respectively, $C_{j'}$) itself. We color the edges of C_j and $C_{j'}$ simultaneously as follows (see Figure 4). First, we choose one edge e of C_j, color e with 2, and color the rival of e with 0. Note that the uncolored edges of C_j form a path Q. Starting at one end of Q, we then color the edges of Q alternatively with colors 0 and 1. Finally, for each uncolored edge e' of $C_{j'}$, we color it with the color $h \in \{1, 2\}$ such that the rival of e' has been colored with $h - 1$. Note that the colored edges satisfy Conditions (C1) through (C3) above.

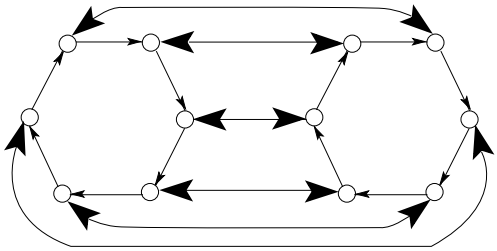


Figure 4: Coloring C_j and $C_{j'}$ when all their edges are critical.

Case 3: Neither Case 1 nor Case 2 occurs and no edge of C_j is a critical dangling edge of H. Then, by Lemma 3.3 and Statement 1 in Lemma 3.5, C contains at least one safe edge. Let e_1, ..., e_k be the edges of C, and assume that they appear in C cyclically in this order. Without loss of generality, we may assume that e_1 is a safe edge. We color e_1 with 0, and then color the edges e_2, ..., e_k in this order as follows. Suppose that we have just colored e_i with a color $h_i \in \{0, 1, 2\}$ and we want to color e_{i+1} next, where $1 \leq i \leq k - 1$. If e_{i+1} is a critical edge and its rival has

been colored with $(h_i + 1)$ mod 3, then we color e_{i+1} with $(h_i + 2)$ mod 3; otherwise, we color e_{i+1} with $(h_i + 1)$ mod 3. If e_k is colored 0 at the end, then we change the color of e_1 from 0 to the color in $\{1, 2\}$ that is not the color of e_2. Now, we can further color each dangling 2-cycle C' of C_j with the color in $\{0, 1, 2\}$ that has not been used to color the two edges of C incident to the articulation vertex of C'. Note that the colored edges satisfy Conditions (C1) through (C3) above.

Case 4: Neither Case 1 nor Case 2 occurs and some edge of C_j is a critical dangling edge of H. For each dangling edge e of H with $e \in E(C_j)$, we define the *partner* of e to be the edge e' of C leaving the articulation vertex u of the dangling 2-cycle containing e, and define the *mate* of e to be the bypass edge e'' of C_j entering u (see Figure 6). We say that an edge e of C_j is *bad* if e is a critical dangling edge of H and its partner is the rival of another critical dangling edge of H. If C_j has a bad edge e, then Statement 3 in Lemma 3.4 ensures that C_j is as shown in Figure 5 and can be colored as shown there without violating Conditions (C1) through (C3) above.

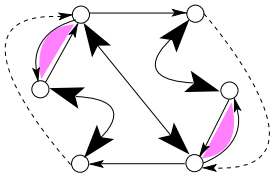


Figure 5: C_j (formed by the one-way edges) and its coloring when it has a bad edge e.

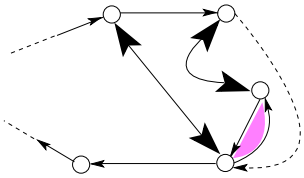


Figure 6: The rival, the mate, and the partner of a critical dangling edge e of H together with the opponent of the partner of e.

So, suppose that C_j has no bad edge. We need one more definition (see Figure 6). Consider a critical dangling edge e of H with $e \in E(C_j)$. Let e' and e'' be the partner and the rival of e, respectively. Let e''' be the edge of C entering the tail of e''. Let P be the open chain in G_2 whose endpoints are the tails of e' and e''. We call e''' the *opponent* of e'. Note that $e' \neq e'''$ because the endpoints of P are the tail of e' and the head of e'''. Moreover, if e' is a critical edge of H, then the rival of e' has to be e''' because e is not bad and P exists. In other words, whenever an edge of C has both its rival and its opponent, they must be the same. Similarly, if e''' is a critical edge of H, then its rival has to be e'. Obviously, neither e' nor E''' can be the rival or the mate of a critical dangling edge of H (because C_j has no bad edge).

Now, let $e_1, \ldots, e_q$ be the edges of C none of which is the rival or the mate of a critical dangling edge of C_j. We may assume that $e_1, \ldots, e_q$ appear in C' cyclically in this order. Without loss of generality, we may further assume that e_1 is the partner of a critical dangling edge of H. Then, we color e_1 with 0, and further color $e_2, \ldots, e_q$ in this order as follows. Suppose that we have just colored e_i with a color $h_i \in \{0, 1, 2\}$ and we want to color e_{i+1} next, where $1 \leq i \leq q - 1$. If e_{i+1} is a critical edge of H and its rival or opponent has been colored with $(h_i + 1)$ mod 3, then we color

e_{i+1} with $(h_i + 2) \bmod 3$; otherwise, we color e_{i+1} with $(h_i + 1) \bmod 3$. Note that the colored edges satisfy Conditions (C1) through (C3) above, because the head of e_q is not the tail of e_1.

We next show how to color the rival and the mate of each critical dangling edge of C_j. For each critical dangling edge e of C_j, since its partner e' and the opponent of e' have been colored, we can color the rival of e with the color of e' and color the mate of e with a color in $\{0, 1, 2\}$ that is not the color of e'. Note that the colored edges satisfy Conditions (C1) through (C3) above, because e' and its opponent have different colors.

Finally, for each dangling 2-cycle D of C_j, we color the two edges of D with the color in $\{0, 1, 2\}$ that has not been used to color an edge incident to the articulation vertex of D. Note that the colored edges satisfy Conditions (C1) through (C3) above, because the rival of each critical dangling edge e of H has the same color as the partner of e does. This completes the coloring of C_j (and hence H).

We next want to show how to use the coloring to find a large-weight tour in G. For each $i \in \{0, 1, 2\}$, let E_i be the edges of H with color i. Without loss of generality, we may assume that $w(E_0) \geq \max\{w(E_1), w(E_2)\}$. Then, $w(E_0) \geq \frac{1}{3}W_{1,3}$ (see the beginning of this subsection for $W_{1,3}$). Consider the undirected graph $U = (V(G), F_1 \cup F_2)$, where F_1 consists of all edges $\{v_1, v_2\}$ such that (v_1, v_2) or (v_2, v_1) is an edge in E_0, and F_2 consists of all edges $\{v_3, v_4\}$ such that v_3 and v_4 are the endpoints of an open chain in G_2. We further assign a weight to each edge of F_1 as follows. We first initialize the weight of each edge of F_1 to be 0. For each edge $(v_1, v_2) \in E_0$, we then add the weight of edge (v_1, v_2) to the weight of edge $\{v_1, v_2\}$. Note that for each $i \in \{1, 2\}$, each connected component of the undirected graph $(V(G), F_i)$ is a single vertex or a single edge because of Condition (C3) above. So, each connected component of U is a path or a cycle. Moreover, each cycle of U contains at least three edges of F_1 because of Condition (C1) above. For eacy cycle D of U, we mark exactly one edge $\{v_1, v_2\} \in F_1$ in D whose weight is the lightest among all edges $\{v_1, v_2\} \in F_1$ in D. Let E_3 be the set of all edges $(v_1, v_2) \in E_0$ such that $\{v_1, v_2\}$ is marked. Then, $w(E_3) \leq \frac{1}{3}w(E_0)$. Consider the directed graph G_2' obtained from G_2 by adding the edges of $E_0 - E_3$. Obviously, $w(G_2') \geq (W_{1,2} + W_{2,2}) + \frac{1}{9}W_{1,3}$. Moreover, G_2' is a collection of partial chains and hence is 2-path-colorable. So, we can partition the edges of G_2' into two subsets E_1' and E_2' such that both graphs $(V(G), E_1')$ and $(V(G), E_2')$ are subtours of G. The heavier one among the two subtours can be completed to a tour of G of weight at least $\frac{1}{2}(W_{1,2} + W_{2,2}) + \frac{1}{18}W_{1,3} \geq W_2 + \frac{1}{9}W_3$. Combining this with Lemma 3.2, we now have:

Theorem 3.6 *There is a polynomial-time approximation algorithm for* AsymMaxTSP *achieving an approximation ratio of* $\frac{27}{35}$.

4 New Algorithm for Metric SymMaxTSP

Throughout this section, fix an instance (G, w) of metric SymMaxTSP, where G is a complete undirected graph with n vertices and w is a function mapping each edge e of G to a nonnegative real number $w(e)$. Because of the triangle inequality, the following fact holds (see [3] for a proof):

Fact 4.1 *Suppose that $P_1, \ldots, P_t$ are vertex-disjoint paths in G each containing at least one edge. For each $1 \leq i \leq t$, let u_i and v_i be the endpoints of P_i. Then, we can use some edges of G to connect $P_1, \ldots, P_t$ into a single cycle C in linear time such that $w(C) \geq \sum_{i=1}^{t} w(P_i) + \frac{1}{2}\sum_{i=1}^{t} w(\{u_i, v_i\})$.*

Like Hassin and Rubinstein's algorithm (H&R2-algorithm) for the problem, our algorithm computes two tours T_1 and T_2 of G and outputs the one with the larger weight. The first two steps of our algorithm are the same as those of H&R2-algorithm:

1. Compute a maximum-weight cycle cover $\mathcal{C}$. Let $C_1, \ldots, C_r$ be the cycles in G.
2. Compute a maximum-weight matching M in G.

Lemma 4.2 [3] *In linear time, we can compute two disjoint subsets A_1 and A_2 of $\bigcup_{1 \leq i \leq r} E(C_i) - M$ satisfying the following conditions:*

(a) For each $j \in \{1, 2\}$, each connected component of the graph $(V(G), M \cup A_j)$ is a path of length at least 1.

(b) For each $j \in \{1, 2\}$ and each $i \in \{1, \ldots, r\}$, $|A_j \cap E(C_i)| = 1$.

For a technical reason, we will allow our algorithm to use only 1 random bit (so we can easily derandomize it, although we omit the details). The third through the seventh steps of our algorithm are as follows:

3. Compute two disjoint subsets A_1 and A_2 of $\bigcup_{1 \leq i \leq r} E(C_i) - M$ satisfying the two conditions in Lemma 4.2.
4. Choose A from A_1 and A_2 uniformly at random.
5. Obtain a collection of vertex-disjoint paths each of length at least 1 by deleting the edges in A from $\mathcal{C}$; and then connect these paths into a single (Hamiltonian) cycle T_1 as described in Fact 4.1.
6. Let $S = \{v \in V(G) \mid \text{the degree of } v \text{ in the graph } (V, M \cup A) \text{ is } 1\}$ and $F = \{\{u, v\} \subseteq E(G) \mid \{u, v\} \subseteq S\}$. Let H be the complete graph (S, F). Let $\ell = \frac{1}{2}|S|$. (Comment: $|S|$ is even, because of Condition (a) in Lemma 4.2.)
7. Let M' be the set of all edges $\{u, v\} \in F$ such that some connected component of the graph $(V, M \cup A)$ contains both u and v. (Comment: M' is a perfect matching of H because of Condition (a) in Lemma 4.2.)

Lemma 4.3 [3] *Let $\alpha = w(A_1 \cup A_2)/w(\mathcal{C})$. For a random variable X, let $\mathcal{E}[X]$ denote its expected value. Then, $\mathcal{E}[w(F)] \geq \frac{1}{4}(1 - \alpha)(2\ell - 1)w(\mathcal{C})$.*

The next lemma shows that there cannot exist matchings of large weight in an edge-weighted graph where the weights satisfy the triangle inequality:

Lemma 4.4 *For every perfect matching N of H, $w(N) \leq w(F)/\ell$.*

Proof. Let the edges of N be $\{u_1, u_2\}$, $\{u_3, u_4\}$, ..., $\{u_{2\ell-1}, u_{2\ell}\}$.

Case 1: ℓ is odd. For each odd number i with $1 \leq i \leq \ell$, we assign the vertices u_{i+2}, u_{i+3}, ..., $u_{\ell+i}$ of H to the edge $\{u_i, u_{i+1}\}$ of N. For each even number j with $1 \leq j \leq \ell$, we assign the vertices u_1, u_2, ..., u_j, $u_{\ell+j+2}$, $u_{\ell+j+3}$, ..., $u_{2\ell}$ of H to the edge $\{u_{\ell+j}, u_{\ell+j+1}\}$ of N. Note that

each edge in N is assigned exactly $\ell - 1$ vertices of H. For each edge $e_i = \{u_i, u_{i+1}\} \in N$ and each vertex u_h assigned to e_i, we then assign the two edges $\{u_i, u_h\}$ and $\{u_{i+1}, u_h\}$ of H to e_i. Since $w(\{u_i, u_h\}) + w(\{u_{i+1}, u_h\}) \geq w(e_i)$ by the triangle inequality, the total weight of edges assigned to each edge $e_i \in N$ is at least $(\ell - 1)w(e_i)$. Obviously, no edge of N is assigned to itself or another edge of N. Moreover, a simple but crucial observation is that no edge of H is assigned to two or more edges of N. Thus, $w(F - N) \geq (\ell - 1)w(N)$. Hence, $w(N) \leq w(F)/\ell$.

Case 2: ℓ is even. Let $N_1 = \{\{u_1, u_2\}, \{u_3, u_4\}, \ldots, \{u_{n-1}, u_n\}\}$ and $N_2 = N - N_1$. We assume that $w(N_1) \geq w(N_2)$; the other case is similar. For each odd number i with $1 \leq i \leq \ell - 1$, we assign the vertices u_{i+2}, u_{i+3}, $\ldots$, $u_{\ell+i+1}$ of H to the edge $\{u_i, u_{i+1}\}$ of N, and assign the vertices u_1, u_2, $\ldots$, u_{i-1}, $u_{\ell+i+2}$, $u_{\ell+i+3}$, $\ldots$, $u_{2\ell}$ of H to the edge $\{u_{\ell+i}, u_{\ell+i+1}\}$ of N. Note that each edge in N_1 (respectively, N_2) is assigned exactly ℓ (respectively, $\ell - 2$) vertices of H. For each edge $e_i = \{u_i, u_{i+1}\} \in N$ and each vertex u_h assigned to e_i, we then assign the two edges $\{u_i, u_h\}$ and $\{u_{i+1}, u_h\}$ of H to e_i. Since $w(\{u_i, u_h\}) + w(\{u_{i+1}, u_h\}) \geq w(e_i)$ by the triangle inequality, the total weight of edges assigned to each edge $e_i \in N_1$ (respectively, $e_i \in N_2$) is at least $\ell w(e_i)$ (respectively, $(\ell - 2)w(e_i)$). Obviously, no edge of N is assigned to itself or another edge of N. Moreover, a simple but crucial observation is that no edge of H is assigned to two or more edges of N. Thus, $w(F - N) \geq \ell w(N_1) + (\ell - 2)w(N_2) \geq (\ell - 1)w(N)$. Hence, $w(N) \leq w(F)/\ell$. □

The following is our main lemma and will be proved in Section 4.1:

Lemma 4.5 *We can partition $F - M'$ into $2\ell - 2$ perfect matchings M_1, $\ldots$, $M_{2\ell-2}$ of H in linear time satisfying the following condition:*

- *For every natural number q, there are at most $q^2 - q$ matchings M_i with $1 \leq i \leq 2\ell - 2$ such that the graph $(S, M' \cup M_i)$ has a cycle of length at most $2q$.*

Now, the eighth through the thirteenth steps of our algorithm are as follows:

8. Partition $F - M'$ into $2\ell - 2$ perfect matchings M_1, $\ldots$, $M_{2\ell-2}$ of H in linear time satisfying the condition in Lemma 4.5.
9. Let $q = \lceil \sqrt[3]{\ell} \rceil$. Find a matching M_i with $1 \leq i \leq 2\ell - 2$ satisfying the following two conditions:
   (a) The graph $(S, M' \cup M_i)$ has no cycle of length at most $2q$.
   (b) $w(M_i) \geq w(M_j)$ for all matchings M_j with $1 \leq j \leq 2\ell - 2$ such that the graph $(S, M' \cup M_j)$ has no cycle of length at most $2q$.
10. Construct the graph $G'_i = (V(G), M \cup A \cup M_i)$. (Comment: $M_i \cap (M \cup A) = \emptyset$ and each connected component of G'_i is either a path, or a cycle of length $2q + 1$ or more.)
11. For each cycle D in G'_i, mark exactly one edge $e \in M_i \cap E(D)$ such that $w(e) \leq w(e')$ for all $e' \in M_i \cap E(D)$.
12. Obtain a collection of vertex-disjoint paths each of length at least 1 by deleting the marked edges from G'_i; and then connect these paths into a single (Hamiltonian) cycle T_2 as described in Fact 4.1.
13. If $w(T_1) \geq w(T_2)$, output T_1; otherwise, output T_2.

Theorem 4.6 *There is an $O(n^3)$-time approximation algorithm for metric* SymMaxTSP *achieving an approximation ratio of $\frac{7}{8} - O(1/\sqrt[3]{n})$.*

PROOF. Let OPT be the maximum weight of a tour in G. It suffices to prove that $\max\{\mathcal{E}[w(T_1)], \mathcal{E}[w(T_2)]\} \geq (\frac{7}{8} - O(1/\sqrt[3]{n})OPT$. By Fact 4.1, $\mathcal{E}[w(T_1)] \geq (1 - \frac{1}{2}\alpha + \frac{1}{4}\alpha)w(\mathcal{C}) \geq (1 - \frac{1}{4}\alpha)OPT$.

We claim that $|S| \geq \frac{1}{3}n$. To see this, consider the graphs $G_M = (V(G), M)$ and $G_A = (V(G), M \cup A)$. Because the length of each cycle in $\mathcal{C}$ is at least 3, $|A| \leq \frac{1}{3}n$ by Condition (b) in Lemma 4.2. Moreover, since M is a matching of G, the degree of each vertex in G_M is 0 or 1. Furthermore, G_A is obtained by adding the edges of A to G_M. Since adding one edge of A to G_M increases the degrees of at most two vertices, there exist at least $n - 2|A| \geq \frac{1}{3}n$ vertices of degree 0 or 1 in G_A. So, by Condition (a) in Lemma 4.2, there are at least $\frac{1}{3}n$ vertices of degree 1 in G_A. This establishes that $|S| \geq \frac{1}{3}n$. Hence, $\ell \geq \frac{1}{6}n$.

Now, let x be the number of matchings M_j with $1 \leq j \leq 2\ell - 2$ such that the graph $(S, M' \cup M_i)$ has a cycle of length at most $2q$. Then, by Lemmas 4.4 and 4.5, the weight of the matching M_i found in Step 9 is at least $(1 - \frac{x+1}{\ell}) \cdot w(F) \cdot \frac{1}{2\ell-2-x}$. So, $w(M_i) \geq \frac{1}{\ell} \cdot (1 - \frac{\ell-1}{2\ell-2-q^2+q}) \cdot w(F)$ because $x \leq q^2 - q$. Let N_i be the set of edges of M_i marked in Step 11. Then, $w(M_i - N_i) \geq \frac{q}{q+1} \cdot \frac{\ell-q^2+q-1}{\ell(2\ell-2-q^2+q)} \cdot w(F)$. Hence, by Lemma 4.3 and the inequality $\ell \geq \frac{1}{6}n$, we have $\mathcal{E}[w(M_i - N_i)] \geq \frac{1}{4}(1 - \alpha)(1 - O(1/\sqrt[3]{n})w(\mathcal{C})$.

Obviously, $\mathcal{E}[w(T_2)] \geq \mathcal{E}[w(M \cup A)] + \mathcal{E}[w(M_i - N_i)] \geq (\frac{1}{2} - \frac{1}{2n})OPT + \frac{1}{2}\alpha w(\mathcal{C}) + \mathcal{E}[w(M_i - N_i)]$. Hence, by the last inequality in the previous paragraph, $\mathcal{E}[w(T_2)] \geq (\frac{3}{4} + \frac{1}{4}\alpha - O(1/\sqrt[3]{n}))OPT$. Combining this with the inequality $\mathcal{E}[w(T_1)] \geq (1 - \frac{1}{4}\alpha)OPT$, we finally have $\mathcal{E}[\max\{w(T_1), w(T_2)\}] \geq (\frac{7}{8} - O(1/\sqrt[3]{n})OPT$.

The running time of the algorithm is dominated by the $O(n^3)$ time needed for computing a maximum-weight cycle cover and a maximum-weight matching. □

As observed in [3], the subsets A_1 and A_2 in Lemma 4.2 can be computed in $O(\log^3 n)$ time using a linear number of processors. So, our algorithm for metric Max TSP is parallelizable because maximum-weight cycle covers and maximum-weight matchings can be computed by fast parallel algorithms [6, 8]. We omit the details here.

4.1 Partitioning into Perfect Matchings

Let the vertices of H be ∞, 0, 1, ..., $2\ell - 2$, and let the edges of M' be

$$\{\infty, 0\}, \{1, 2\ell - 2\}, \{2, 2\ell - 3\}, \ldots, \{\ell - 1, \ell\}.$$

Then, a folklore partitioning of $F - M'$ into $2\ell - 2$ perfect matchings M_1, ..., $M_{2\ell-2}$ of H is as follows:

$$M_1 : \{\infty, 1\}, \{2, 0\}, \{3, 2\ell - 2\}, \ldots, \{\ell, \ell + 1\}$$

$$M_2 : \{\infty, 2\}, \{3, 1\}, \{4, 0\}, \ldots, \{\ell + 1, \ell + 2\}$$

$$\vdots$$

$$M_{2\ell-2} : \{\infty, 2\ell - 2\}, \{0, 2\ell - 3\}, \{1, 2\ell - 4\}, \ldots, \{\ell - 2, \ell - 1\}.$$

For each integer $j \notin \{0, 1, \ldots, 2\ell - 2\}$, we identify j with the vertex h of H such that $h \equiv j \pmod{2\ell - 1}$. Then, for each integer $i \in \{0, 1, \ldots, 2\ell - 2\}$, M_i consists of edge $\{\infty, i\}$ and all

edges $\{j, -j+2i\}$ with $j \in \{0, 1, \ldots, 2\ell-2\} - \{i\}$. Obviously, for each $i \in \{1, \ldots, 2\ell-2\}$, the graph $H_i = (S, M_i \cup M')$ is a collection of vertex-disjoint cycles; we call the cycle containing vertex ∞ the *main cycle* of H_i and denote it by D_i. For two natural numbers x and y, let $\gcd(x, y)$ denote the greatest common divisor of x and y, and let $\mathrm{lcm}(x, y)$ denote the least common multiple of x and y.

Lemma 4.7 *For each $i \in \{1, \ldots, 2\ell-2\}$, the length of D_i is $\left(\frac{2\ell-1}{\gcd(2\ell-1,i)} + 1\right)$.*

Proof. Recall that for each integer $i \in \{0, 1, \ldots, 2\ell-2\}$, M_i consists of edge $\{\infty, i\}$ and all edges $\{j, -j+2i\}$ with $j \in \{0, 1, \ldots, 2\ell-2\} - \{i\}$. Fix an $i \in \{1, \ldots, 2\ell-2\}$. Let $2h$ be the length of D_i. Suppose that we traverse D_i by starting at vertex ∞, then visiting i, and proceeding along the cycle until reaching vertex 0. This traversal should give the following ordering of the vertices of D_i:

$$\infty, i, -i, 3i, -3i, 5i, \cdots, -(2h-3)i, (2h-1)i$$

where $(2h-1)i \equiv 0 \pmod{2\ell-1}$ because vertex 0 is the last one in the traversal. Note that for every odd $x \in \{1, 2, \ldots, 2h-1\}$, xi is a vertex of D_i.

Since $(2h-1)i \equiv 0 \pmod{2\ell-1}$, $(2h-1)i$ is a common multiple of integers $2\ell-1$ and i, and hence there exists an integer $\alpha \geq 1$ such that

$$(2h-1)i = \alpha \,\mathrm{lcm}(2\ell-1, i) = \left(\alpha \cdot \frac{2\ell-1}{\gcd(2\ell-1, i)}\right) i. \tag{4.1}$$

The last equality follows from the fact that $(2\ell-1)\, i = \gcd(2\ell-1, i)\, \mathrm{lcm}(2\ell-1, i)$. By Equation 4.1, $2h-1 = \alpha \cdot \frac{2\ell-1}{\gcd(2\ell-1,i)}$. Therefore, α is an odd integer because $\frac{2\ell-1}{\gcd(2\ell-1,i)}$ is an integer and $2h-1$ is odd.

We claim that $\alpha = 1$. For a contradiction, assume that α is an odd integer greater than 1. Then, by Equation 4.1, $(2h-1)i - (\alpha-1)\,\mathrm{lcm}(2\ell-1, i) = \mathrm{lcm}(2\ell-1, i)$ and hence

$$2h - 1 - (\alpha-1) \cdot \frac{2\ell-1}{\gcd(2\ell-1, i)} = \frac{\mathrm{lcm}(2\ell-1, i)}{i}. \tag{4.2}$$

Since $\alpha - 1$ is a possitive even integer, the left side of Equation 4.2 is an odd integer less than $2h-1$. Moreover, recall that $2h-1 = \alpha \cdot \frac{2\ell-1}{\gcd(2\ell-1,i)}$. So, the left side of Equation 4.2 is a positive odd integer less than $2h-1$. Hence, $(2h-1-(\alpha-1) \cdot \frac{2\ell-1}{\gcd(2\ell-1,i)})\, i$ is an integer in the subsequence i, $3i$, $5i$, $\ldots$, $(2h-3)i$, and is a multiple of $2\ell-1$ by Equation 4.2. However, this implies that vertex 0 of D_i is in the subsequence i, $3i$, $5i$, $\ldots$, $(2h-3)i$, a contradiction. Thus, the claim holds.

By the claim, $2h-1 = \frac{2\ell-1}{\gcd(2\ell-1,i)}$ and so the length of D_i is $2h = \frac{2\ell-1}{\gcd(2\ell-1,i)} + 1$. □

Corollary 4.8 *If $\gcd(2\ell-1, i) = 1$, then D_i is a tour of H_i.*

We next show that if D_i is not a tour of H_i, then D_i is the shortest cycle in H_i.

Lemma 4.9 *Fix an i such that $1 \leq i \leq 2\ell-2$ and $\gcd(2\ell-1, i) \neq 1$. Then, each cycle of H_i other than D_i is of length $\frac{2(2\ell-1)}{\gcd(2\ell-1,i)}$.*

PROOF. Fix a cycle D of H_i other than D_i. Let $2h$ be the length of D. Consider an arbitrary vertex j of D. As in the proof of Lemma 4.7, a traversal of D started at vertex j and ended at vertex $-j$ produces the following ordering of the vertices of D:

$$j, -j+2i, j-2i, -j+4i, j-4i, -j+6i, \ldots, j-2(h-1)i, -j+2hi$$

where $-j+2hi \equiv -j \pmod{2\ell-1}$. Note that for every even $x \in \{2,3,\ldots,2h\}$, $-j+xi$ is a vertex of D.

Since $2hi \equiv 0 \pmod{2\ell-1}$, $2hi$ is a common multiple of integers $2\ell-1$ and i, hence there exists an integer $\alpha \geq 1$ such that

$$2hi = \alpha \operatorname{lcm}(2\ell-1, i) = \left(\alpha \cdot \frac{2\ell-1}{\gcd(2\ell-1, i)}\right) i. \tag{4.3}$$

By Equation 4.3, $2h = \alpha \cdot \frac{2\ell-1}{\gcd(2\ell-1,i)}$. Therefore, α is an even integer.

We claim that $\alpha = 2$. For a contradiction, assume that α is an even number greater than 2. Then, by Equation 4.3, $2hi - (\alpha-2)\operatorname{lcm}(2\ell-1,i) = 2\operatorname{lcm}(2\ell-1,i)$ and hence

$$2h - (\alpha-2) \cdot \frac{2\ell-1}{\gcd(2\ell-1,i)} = \frac{2\operatorname{lcm}(2\ell-1,i)}{i}. \tag{4.4}$$

Since $\alpha-2$ is a possitive even integer, the left side of Equation 4.4 is an even integer less than $2h$. Moreover, recall that $2h = \alpha \cdot \frac{2\ell-1}{\gcd(2\ell-1,i)}$. So, the left side of Equation 4.4 is a positive even integer less than $2h$. Hence, $-j + (2h - (\alpha-2) \cdot \frac{2\ell-1}{\gcd(2\ell-1,i)})\, i$ is an integer in the subsequence $-j+2i$, $-j+4i$, $\ldots$, $-j+2(h-1)i$, and is congruent to $-j$ modulo $2\ell-1$ by Equation 4.4. However, this implies that vertex $-j$ of D_i is in the subsequence $-j+2i$, $-j+4i$, $\ldots$, $-j+2(h-1)i$, a contradiction. Thus, the claim holds.

By the claim, $2h = \frac{2(2\ell-1)}{\gcd(2\ell-1,i)}$ and so the length of D_i is $2h = \frac{2(2\ell-1)}{\gcd(2\ell-1,i)}$. □

Corollary 4.10 *For every $i \in \{1,2,\ldots,2\ell-2\}$, D_i is the shortest cycle in H_i.*

PROOF. Fix an $i \in \{1,2,\ldots,2\ell-2\}$. If $\gcd(2\ell-1,i) = 1$, then D_i is the unique cycle (and hence the shortest cycle) in H_i by Corollary 4.8. Otherwise, by Lemmas 4.7 and 4.9, D_i is shorter than the other cycles in H_i. □

Now, we are ready to prove Lemma 4.5:

PROOF OF LEMMA 4.5: Fix a natural number q. By Corollary 4.10, it suffices to show that there are at most q^2-q integers $i \in \{1,2,\ldots,2\ell-2\}$ such that D_i is of length at most $2q$.

Consider a natural number $p \leq q$. For each $i \in \{1,2,\ldots,2\ell-2\}$, if the length of D_i is exactly $2p$, then by Lemma 4.7, $\frac{2\ell-1}{\gcd(2\ell-1,i)} + 1 = 2p$ and so

$$\gcd(2\ell-1, i) = \frac{2\ell-1}{2p-1}.$$

Since each integer i satisfying the above equality has to be a multiple of $\frac{2\ell-1}{2p-1}$, there can be at most $2p-2$ such integers in $\{1,2,\ldots,2\ell-2\}$.

Hence, there can be at most $\sum_{p=1}^{q}(2p-2) = q^2-q$ integers $i \in \{1,2,\ldots,2\ell-2\}$ such that H_i has a cycle of length at most $2q$. □

References

[1] A. I. Barvinok, D. S. Johnson, G. J. Woeginger, and R. Woodroofe. Finding Maximum Length Tours under Polyhedral Norms. *Proceedings of the Sixth International Conference on Integer Programming and Combinatorial Optimization* (IPCO), Lecture Notes in Computer Science, **1412** (1998) 195–201.

[2] Z.-Z. Chen and L. Wang. An Improved Randomized Approximation Algorithm for Max TSP. *Submitted*.

[3] Z.-Z. Chen, Y. Okamoto, and L. Wang. Improved Deterministic Approximation Algorithms for Max TSP. *Submitted*.

[4] R. Hassin and S. Rubinstein. A 7/8-Approximation Approximations for Metric Max TSP. *Information Processing Letters*, **81** (2002) 247–251.

[5] H. Kaplan, M. Lewenstein, N. Shafrir, and M. Sviridenko. Approximation Algorithms for Asymmetric TSP by Decomposing Directed Regular Multigraphs. *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science*, pp. 56–75, 2003.

[6] R. M. Karp, E. Upfal, and A. Wigderson. Constructing a Perfect Matching is in random NC. *Combinatorica*, **6** (1986) 35–48.

[7] A. V. Kostochka and A. I. Serdyukov. Polynomial Algorithms with the Estimates $\frac{3}{4}$ and $\frac{5}{6}$ for the Traveling Salesman Problem of Maximum (in Russian). *Upravlyaemye Sistemy*, **26** (1985) 55–59.

[8] K. Mulmuley, U. V. Vazirani, and V. V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, **7** (1987) 105–113.

Proposal of Asynchronous Distributed Branch and Bound(Abstract)

[1] Atsushi SASAKI [1] Tadashi ARARAGI [2] Shigeru MASUYAMA
[1]NTT CSL [2] Toyohashi University of Technology

This talk proposes new asyncronous distributed branch and bound. This is the first algorithm to provide the exact optimum solution, not an approximation, for NP-hard distributed system in a distributed context without any centralized control. Moreover, this algorithm has more flexibility and greater robustness than the conventional distributed algorithms without any centralized control. The idea behind the algorithm is a complex consisting of branch and bound, divide and conquer, and λ-opt neighborhood in local search. This algorithm is promising for wide-range of applications in an actual huge dynamic distributed system.

Load balancing, resource allocation, and location problems are essential for robust, flexible, and efficient operations in distributed systems. Many of these discrete optimization problems are NP-hard and a number of studies have investigated these problems in both sequential and distributed contexts. As regards optimization, only a few studies have been conducted on distributed systems, whereas sequential systems have been studied extensively. We think that this is due to the difficulty involved in optimizing actual huge distributed systems. Almost all distributed approximation schemes can be recognized as a kind of local search. This is because only local information, not global information, is available in the scheme. In such a scheme, if the initial state is a local minimum or it reaches a local minimum, the system performance cannot be further improved. Therefore, optimization is required even though the problem is NP-hard and it must also be used as an approximation schemes. Moreover, in geographically distributed systems, fault tolerance, adaptation for dynamics (e.g., dynamic task arrival), and usability in huge systems are also required and are sometimes more important than efficiency from the viewpoint of flexibility and robustness. A new distributed branch and bound algorithm we propose here has the potential to satisfy all of these requirements. In this talk, we propose only the most fundamental framework of asynchronous distributed branch and bound. Therefore, further work on this framwork will make it more useful.

Although branch and bound is a fundamental framework for solving discrete optimization problems by enumeration in sequential contexts, there have only been two studies, as far as we know, branch and bound in distributed contexts, namely, synchronous branch and bound and distributed branch and bound. The former simply simulates the sequential branch and bound in a distributed context. The latter is summarized as follows: A host gathers all the information about a problem and then begins the execution of branch and bound. Basically, the algorithm works so that the host assigns each subproblem to another host. That is, the latter is a simple distributed version of sequential branch and bound. These algorithms do not consider fault tolerance or adaptation for dynamics, and so lack robustness and flexibility. Moreover, these algorithms need some kind of centralized control, which also results in a lack of robustness and flexibility.

The algorithm proposed in this talk, called asynchronous distributed branch and bound, is another distributed version of branch and bound. However, this also incorporates ideas from other schemes. In fact, this algorithm includes the idea of divide and conquer and that of optimization with respect to local search (λ-opt neighborhood). That is, at a first glance the proposed algorithm looks very different from the sequential branch and bound. The main difference is that sequential branch and bound is based on exactly one branching tree, while the proposed algorithm maintains more than one branching tree, that is, each host has a branching tree maintained independently (asynchronously).

We first discuss the features of the target problmes, especially for the load balancing. We then summarize the requirements for algorithms designed to solve the problems in a geographically distributed system. We propose a new asynchronous distributed framework and then prove its correctness.

Energy-Optimal Online Algorithms for Broadcasting in Wireless Networks

Shay Kutten*, Hirotaka Ono†, David Peleg‡,
Kunihiko Sadakane†, and Masafumi Yamashita†

We consider problems related to the design of energy-efficient online message broadcasting protocols in ad-hoc wireless networks. Recent developments in portable wireless devices with limited power resources have led to considerable interest in problems involving the construction of energy-efficient multicast trees in the network. Wireless devices can control their transmission power in order to save power consumption whenever the distance to the intended destination of the transmission is known. The attenuation of a signal with power P_s is $P_r = \frac{P_s}{d(s,t)^\delta}$, where $d(s,t)$ is the distance between hosts s and t, and $\delta \geq 1$ is the *distance-power gradient* [3]. A message can be successfully decoded if P_r is no less than a constant γ. Therefore the *transmission range* of a host s, namely, the maximum distance to which a message can be successfully delivered from s, is $(P_s/\gamma)^{1/\delta}$. Power control also has a positive effect on reducing the number of transmission collisions between nearby senders.

The problem studied here concerns a single sender which has to transmit a message to a given collection of receivers in an online setting, namely, when the hosts do not know each other's locations. The goal is to specify a protocol for the sender allowing it to directly broadcast the message to the recipients and receive acknowledgements, while minimizing the total transmission costs. By *direct broadcast* we mean that the sender is required to transmit the message itself to every recipient, namely, multi-hop delivery is not allowed. This restriction may be relevant in situations when the battery resources of the receivers is severely limited and it is desired to minimize their transmissions, or when when the reliability of the hosts is uncertain and only direct messages from the source can be trusted.

Using varying levels of transmission power is important for energy-efficient communication. As far as the authors are aware, there has been no online algorithms with provable worst-case guarantees for energy-efficient broadcasting in ad-hoc wireless networks.

The protocols proposed in this study are based on computing or estimating the distances from the sender host to the receiver hosts in an energy-efficient way. The most

*Information Systems Group, Faculty of Industrial Engineering and Management, Technion, Haifa, Israel. kutten@ie.technion.ac.il

†Department of Computer Science and Communication Engineering, Kyushu University, Fukuoka, Japan. {ono,sada,mak}@csce.kyushu-u.ac.jp

‡Department of Computer Science and Applied Mathematics, The Weizmann Institute of Science, Rehovot, Israel. david.peleg@weizmann.ac.il

basic case is that of a single sender and a single receiver. The generic doubling protocol employed by the sender is based on repeatedly transmitting the messages to increasingly larger distances, until reaching the receiver. The behavior of this protocol depends on the choice of the sequence of distances, and the problem is to determine them so as to minimize the overall power consumption. If a specific probability distribution may be assumed on the hosts, the algorithm can be optimized [4]. However we assume an online setting in which no a priori information is given about the distance from the sender to the receiver. Therefore the worst-case scenario should be considered. This motivation leads us to apply a competitive analysis to the algorithm (cf. [2]). We compare the power consumption of an algorithm with that of the optimal (infeasible) offline algorithm that knows the distance d. We show that the optimal competitive ratio for this problem is $3/2+\sqrt{2}$, i.e., there exists an online algorithm for the problem with this competitive ratio, and no online algorithm has smaller competitive ratio. The problem is somewhat similar to the famous *cow path* online problem [1], but setting the parameter of the algorithm is not obvious.

Furthermore, we study the generalization of this problem where there is more than one receiver. This is a propoer extension of the cow path problem. For this problem we also propose a competitive online algorithm and prove its optimality. Interestingly, the competitive ratio of the generalized problem is the same, namely, $3/2 + \sqrt{2}$.

References

[1] R. Baeza-Yates, J. Culberson and G. Rawlins, Searching in the plane. *Information and Computation* 106:234–252, 1993.

[2] A. Borodin and R. El-Yaniv, *Online Computation and Competitive Analysis*, Cambridge Univ. Press, 1998.

[3] G.S. Lauer. *Packet radio routing*, Chapt. 11, *Routing in communication networks*, M. Streenstrup (ed.), pages 351–396. Prentice-Hall, 1995.

[4] R. Mathar and J. Mattfeldt. Optimal Transmission Ranges for Mobile Communication in Linear Multihop Packet Radio Networks. *Wireless Networks*, 2:329–342, 1996.

Site-oriented Framework for Mining Communities on the Web

Yasuhito Asano

Graduate School of Information Sciences, Tohoku University.
Aza-Aoba 6-6-05, Aramaki, Aoba-ku, Sendai, Japan 980-8579.
asano@nishizeki.ecei.tohoku.ac.jp

The World Wide Web has evolved at a surprisingly high speed both in its size and in the variety of its contents. There are several methods for mining communities, a set of related pages or sites, on the Web using hyperlinks. Well-known examples of such methods include Kleinberg's HITS [4], trawling proposed by Kumar *et al.* [5], and the max-flow based method proposed by Flake *et al.* [3]. These methods adopt a page-oriented framework, that is, it uses a page on the Web as a unit of information. However, not a page but a site is frequently considered as a unit of information in the Web.

In this talk, we introduce a site-oriented framework for mining communities and our implementation of the site-oriented framework; for the implementation, we propose a new model of sites, called directory-based sites, and establish a method of identifying directory-based sites from data of URLs and links. We explain why our site-oriented framework is more suitable for mining communities than the page-oriented framework, by presenting several theoretical evidences and the results of computational experiments using trawling, the max-flow based method, and our new method which enumerates maximal cliques of *mutual-links*.

This talk is primarily based on the contents of the references [1] and [2].

References

[1] Y. Asano. *A new framework for link-based formation retrieval from the Web.* Ph.D. thesis, The Graduate School of Science, the University of Tokyo, March 2003.

[2] Y. Asano, H. Imai, M. Toyoda, and M. Kitsuregawa, "Finding neighbor communities in the Web using an inter-site graph," IEICE Trans. Inf. Syst., Vol. E87-D, No. 9, pp. 2163-2170, 2004.

[3] G. W. Flake, S. Lawrence, and C. L. Giles, "Efficient identification of Web communities," Proc. 6th International Conference on Knowledge Discovery and Data Mining (ACM SIGKDD-2000), pp.150–160, 2000.

[4] J. Kleinberg. Authoritative sources in a hyperlinked environment. *Proc. of the 9th Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 668–677, 1998.

[5] R. Kumar, P. Raghavan, S. Rajagopalan, and A. Tomkins. Trawling the Web for emerging cyber-communities. *Computer Networks* 31(11-16), pp. 1481–1493, 1999.

On Right-Hand-on-the-Wall Traversal of Graphs

Kunihiko Sadakane

Department of Computer Science
and Communication Engineering

Kyushu University

Hakozaki 6-10-1, Higashi-ku, Fukuoka 812-8581, Japan
sada@csce.kyushu-u.ac.jp

We consider the problem of assigning edge labels to a simple connected graph satisfying the following three conditions: (1) Each edge has two integer labels, one for each end. (2) For each vertex v of the graph, the labels around it are distinct and between 1 and d_v where d_v is the degree of v. (3) There exists a cycle visiting all the vertices which starts from an edge with label 1 around a vertex, and each time we arrive a vertex v from an edge with label i, we go to the edge with label $i+1 \pmod{v_d}$. This problem has applications of efficient broadcasting in networks using less memory. We first show that for any graph, there exists an assignment of labels satisfying the above conditions. Then we consider lower and upper bounds of the length of cycles.

Distributing Distinct Integers Uniformly over a Square Matrix with Application to Digital Halftoning

Boris Aronov[1] Tetsuo Asano[2], Sunseong Choe[2], Shinya Hashima[2], Yosuke Kikuchi[3], Subhas C. Nandy[4], Shinji Sasahara[5], Shao-Chin Sung[2], and Takeaki Uno[6]

[1] Polytechnic University, U.S.A.
[2] School of Information Science, Japan JAIST,
[3] ERATO QCI Project, Japan JST,
[4] Indian Statistical Institute, India
[5] Fuji Xerox Co., Ltd., Japan
[6] National Institute of Informatics (NII), Japan

A *semimagic square* is an $n \times n$ matrix filled with the numbers $0, \ldots, n^2 - 1$ in such a way that the sum of the numbers in each row and each column are the same. Magic squares and related classes of integer matrices have been studied extensively.

In this talk we generalize the notion of a semimagic square by replacing the requirement that all row and column sums be the same by the analogous requirement for all $k \times k$ contiguous square submatrices; we call such $n \times n$ matrices *zero $k \times k$-discrepancy matrices* of order (k, n). Let $\mathbb{N}(k, n)$ be the set of all such matrices. In this talk we show that $\mathbb{N}(k, n)$ is non-empty if k and n are both even, and empty if they are relatively prime. Further, we show by an explicit construction that $\mathbb{N}(k, k^m) \neq \emptyset$ for any integers $k, m \geq 2$.

It is known that it is impossible to achieve zero discrepancy when n is odd and k is 2, but it is not known how small the discrepancy can be for such n and k. In this talk, we present a scheme for achieving a new discrepancy bound $2n$ for the case. This is an improvement from the previous bound $4n$.

Our investigation is motivated by an application described below, but intuitively we seek a matrix filled with distinct integers in an as uniform a manner as possible. The analogous geometric problem of distributing n points uniformly in a unit square has been studied extensively in the literature [2, 3]. Usually, a family of regions is introduced to evaluate the uniformity of a point distribution. If the points of an n-point set P are uniformly distributed, for any region R in the family the number of points in R should be close to $\frac{1}{n}\text{area}(R)$, where $\frac{1}{n}$ is the point density of P in the entire square. Thus, the *discrepancy of P in a region R* is defined as the difference between this value and the actual number of points of P in R. The *discrepancy of the point distribution P* with respect to the family of regions is defined by the maximum such difference, over all regions. In the context of digital halftoning, a family of axis-parallel squares (contiguous square submatrices) over a matrix is appropriate for measuring the uniformity since human eye perception is usually modeled using weighted sum of intensity levels with Gaussian coefficients over square regions around each pixel [1]. Thus, the matrices discussed in this paper can be used as dither matrices in which integers are arranged in an apparently random manner to be used as variable thresholds.

References

1. T. Asano, "Digital Halftoning: Algorithm Engineering Challenges," *IEICE Trans. on Inf. and Syst.*, E86-D, 2, 159–178, 2003.
2. B. Chazelle: *The Discrepancy Method: Randomness and Complexity*, Cambridge University Press, 2000.
3. J. Matoušek: *Geometric Discrepancy*, Springer, 1991.

Ultimate Implementation and Analysis of the AMO Algorithm for Pricing European-Asian Options

Akiyoshi Shioura (Tohoku University) Takeshi Tokuyama (Tohoku University)

We consider the pricing of European-Asian option which is a kind of path-dependent options. The payoff of a European-Asian option is given as $(A - X)^+$, where A is the average stock price during the time from the purchase date to the expiration date of the option and X is the strike price. It is known to be #P-hard in general to compute the exact price of path-dependent options on the binomial tree model. Therefore, it is desired to design an efficient approximation algorithm with provable high accuracy, and various pricing techniques have been developed so far.

A naive method for computing the exact price of European-Asian options, called the full-path method, enumerates all paths in the binomial tree model. Unfortunately, the full-path method requires exponential time since there are exponential number of paths in the binomial tree.

Aingworth, Motwani, and Oldham (AMO) (2000) proposed the first polynomial-time approximation algorithm with guaranteed worst-case error bound, which enables us to avoid the influence of volatility to the theoretical error bound. The idea is to prune exponential number of high-payoff paths by using mathematical formulae during the run of an aggregation algorithm based on dynamic programming and bucketing. In each of n aggregation steps the algorithm produces the error bounded by X/k, where k denotes the number of buckets used at each node of the binomial tree. Hence, the error bound of the AMO algorithm is nX/k, and the algorithm runs in $\mathrm{O}(kn^2)$ time.

The error bound is improved by Dai et al. (2002) and by Ohta et al. (2002). While the AMO algorithm uses the same number of buckets at each node of the binomial tree, Dai et al. use different number of buckets at each node. By adjusting the number of buckets at each node appropriately while keeping the time complexity $\mathrm{O}(kn^2)$, they achieved the error bound $\mathrm{O}(\sqrt{n}X/k)$, where k is the average number of buckets used at each node. On the other hand, Ohta et al. use the idea of randomized rounding in the aggregation steps of the algorithm, and achieves the error bound $\mathrm{O}(n^{1/4}X/k)$.

In this talk, we further reduce the error bound by giving a randomized approximation algorithm with an $\mathrm{O}(kn^2)$ time complexity and an $\mathrm{O}(X/k)$ error bound. The error bound of our algorithm is independent of the depth n of the binomial tree, although those of the AMO algorithm and its previous variants are dependent on n. Our algorithm uses the ideas in Dai et al. (2002) and Ohta et al. (2002). As in Ohta et al. (2002), we regard the aggregation steps of the algorithm as a Martingale process with $\mathrm{O}(n^2)$ random steps by using novel random variables. It can be shown that the expected value of the output by our algorithm equals the exact price, and that the error in each single step is bounded by a function of the number of buckets at a node of the binomial tree. Thus, we can apply Azuma's inequality to the Martingale process to obtain the error bound. If we choose k as the number of buckets at each node, the algorithm coincides with the one by Ohta et al. To reduce the error bound as much as possible, we adjust the number of buckets at each node and obtain the error bound $\mathrm{O}(X/k)$, where k is the average number of buckets used at each node. Since the value X/k can be seen as the "average" of the absolute error produced at each node of the binomial tree, the error bound of our algorithm is the best possible within the framework of the AMO algorithm. We also show the practical quality of the approximate value computed by our algorithm by some numerical experiments.

Algorithms for Modern Memory Systems

Martin Farach-Colton
Department of Computer Science
Rutgers University
USA

For indexing large external-memory ("on disk") data, B-trees and their variants [1, 4] have been the data structures of choice for over three decades, primarily because B-trees minimize the number of disk-block accesses during a search. B-trees, however, are known to be empirically suboptimal because they exploit data locality at only one level of granularity (typically disk blocks), but not at courser or finer granularities.

Traditionally, external-memory algorithms have been analyzed in the so-called *Disk Access Machine (DAM) Model* [6], an idealized two-level memory model in which all block transfers have unit cost, the block size is B, and the main-memory size is M. The choice of B defines the single granularity of data locality of such data structures. For example, a B-tree has a branching factor of B, and thus performs $O(\log_B N)$ memory transfers for queries and updates, which is optimal within the DAM model. Although B is often thought of as a disk-block size, the DAM model applies equally well to optimizing cache-misses, in which case B is taken to be the cache-line size. The widespread use of B-trees suggests that the DAM model is used implicitly as a simplifying approximation for writing memory-oriented code.

The *cache-oblivious* (CO) model [5] is a parameter-free alternative to the *disk-access machine* (DAM) model. As with the DAM model, the objective is to minimize the number of data transfers between two levels. However, unlike the DAM model, the parameters B, the block size, and M, the main-memory size, are unknown to the coder or the algorithm. The main idea of the CO model is that if it can be proved that some algorithm performs a nearly optimal number of memory transfers in a two-level model with unknown parameters, then the algorithm also performs a nearly optimal number of memory transfers on any unknown, multilevel memory hierarchy. Thus, for example, an optimal Cache-oblivious B-trees [3] simultaneously optimizes for both cache misses and page faults. Note, however, that CO algorithms are not self-adjusting. Rather, they are optimized for every level of granularity throughout their execution without any tuning.

Cache obliviousness has been considered a theoretical curiosity. The standard reasoning is that one must loose some performance by ignoring memory parameters, though it has been

shown that many problems can be solved with only a loss of a small constant compared to the best cache-aware algorithm.

In this talk, we suggest the opposite. There are good reasons to believe that cache-oblivious algorithms can outperform cache-aware algorithms. We show theoretical and experimental [2] justification for this claim.

References

[1] R. Bayer and E. M. McCreight. Organization and maintenance of large ordered indexes. *Acta Informatica*, 1(3):173–189, Feb. 1972.

[2] M. Bender, M. Farach-Colton, and B. Kuszmaul. Cache-oblivious B-trees for optimizing disk performance. Submitted for publication, December 2004.

[3] M. A. Bender, E. Demaine, and M. Farach-Colton. Cache-oblivious B-trees. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 399–409, 2000.

[4] D. Comer. The ubiquitous B-tree. *ACM Computing Surveys*, 11(2):121–137, June 1979.

[5] M. Frigo, C. E. Leiserson, H. Prokop, and S. Ramachandran. Cache-oblivious algorithms. In *40th Annual Symposium on Foundations of Computer Science*, pages 285–297, New York, New York, Oct. 17–19 1999.

[6] J. S. Vitter. External memory algorithms. *Lecture Notes in Computer Science*, 1461, 1998.

Data Stream Algorithms and Applications

Shan Muthukrishnan
Rutgers University

In the data stream scenario, input arrives very rapidly and there is limited memory to store the input. In the past few years, researchers in Theoretical Computer Science, Databases, IP Networking and Computer Systems have developed new algorithms that work within these space and time constraints. The methods rely on metric embeddings, pseudo-random computations and sparse approximation theory. The applications include IP network traffic analysis, mining text message streams for Homeland Security and processing massive data sets in general.

I will present an overview of the principles, one or two key technical results and discuss issues in building data stream systems that work at the speed of IP routers. I will also discuss open problems. This talk is based on an updated version of the survey at `http://www.cs.rutgers.edu/~muthu/stream-1-1.ps`

On Computing all Abductive Explanations from a Propositional Horn Theory

Kazuhisa Makino
Osaka University

Abduction is a fundamental mode of reasoning, which has applications in many areas of AI and Computer Science. The computation of abductive explanations is an important computational problem, which is at the core of early systems such as the ATMS and Clause Management Systems, and is intimately related to prime implicate generation in propositional logic. In this talk, we consider the problem of computing multiple explanations, and in particular all explanations for an abductive query from a propositional Horn theory. Our study pays particular attention to the form of the query, ranging from a literal to a compound formula, to whether explanations are based on a set of abducible literals, and to the representation of the Horn theory, either by a Horn CNF or model-based in terms of its characteristic models. For all these combinations, we present either tractability results in terms of polynomial total-time algorithms, intractability results in terms of nonexistence of such algorithms (unless P=NP), or semi-tractability results in terms of solvability in quasi-polynomial time, established by polynomial- time equivalence to the problem of dualizing a monotone conjunctive normal form expression. Our results complement previous results in the literature, and refute a longstanding conjecture by Selman and Levesque. They elucidate the complexity of generating all abductive explanations, and shed light on the related problems such as generating sets of restricted prime implicates of a Horn theory. The algorithms for tractable cases can be readily applied for generating a polynomial subset of explanations in polynomial time. (Joint work with Thomas Eiter)

How to Influence Noncooperative, Selfish Agents

Lisa K. Fleischer
IBM

The societal value of a distribution of finite resources is frequently measured in terms of of aggregate utility. Decisions, however, are frequently controlled by noncooperative agents who try to maximize their own private utility. Papadimitriou coined the term "price of anarchy" to refer to the ratio of social utility achieved by selfish agents versus the social optimal.

In network routing games, the price of anarchy can be arbitrarily bad. We review these results, and then describe some solutions to prevent this bad outcome. These include charging users for network use; and managing a small portion of traffic wisely. Some of these results carry over to more general congestion games.

Metric Labeling: Upper and Lower Bounds

Seffi Naor
Computer Science Dept., Technion
Haifa, Israel

The Metric Labeling problem is an elegant and powerful mathematical model capturing a wide range of classification problems that arise in computer vision and related fields. In a typical classification problem, one wishes to assign labels to a set of objects to optimize some measure of the quality of the labeling. The metric labeling problem captures a broad range of classification problems where the quality of a labeling depends on the pairwise relations between the underlying set of objects, as described by a weighted graph. Additionally, a metric distance function on the labels is defined, and for each label and each vertex, an assignment cost is given. The goal is to find a minimum-cost assignment of the vertices to the labels. The cost of the solution consists of two parts: the assignment costs of the vertices and the separation costs of the edges (each edge pays its weight times the distance between the two labels to which its endpoints are assigned). Note that if the distance function d is not a metric, then determining whether a graph can be colored by k colors is a special case of the labeling problem.

Metric labeling has many applications as well as rich connections to some well known problems in combinatorial optimization. It is related to the *quadratic assignment* problem, an extensively studied problem in Operations Research. A special case of metric labeling is the *0-extension* problem. There are no assignment costs in this problem, however, the graph contains a set of terminals, $t_1, \ldots, t_k$, where the label of terminal t_i is fixed in advance to i, and the non-terminals are free to be assigned to any of the labels. As in the metric labeling problem, a metric is defined on the set of labels. Clearly, the 0-extension problem generalizes the well-studied *multi-way cut* problem in which the metric on the label set is the uniform metric.

In the talk I will discuss the rich body of work in approximation algorithms, as well as lower bounds on approximability, that has been developed in recent years for the metric labeling problem and its variants.

Approximate distance oracles and spanners with sublinear error terms

Speaker: Uri Zwick *

Abstract

Several years ago, Thorup and Zwick obtained the following result: Let $G = (V, E)$ be an undirected *weighted* graph with $|V| = n$ and $|E| = m$. Let $k \geq 1$ be an integer. Then, $G = (V, E)$ can be preprocessed in $O(kmn^{1/k})$ expected time, constructing a data structure of size $O(kn^{1+1/k})$, such that any subsequent *distance query* can be answered, approximately, in $O(k)$ time. The approximate distance returned of stretch at most $2k - 1$, i.e., it is at most $2k - 1$ times the actual distance, and it is never too small. A girth conjecture of Erdős implies that $\Omega(n^{1+1/k})$ space is needed in the worst case for any stretch strictly smaller than $2k + 1$. The space requirement of our algorithm is, hence, essentially optimal.

We now show that the techniques used to construct approximate distance oracles mentioned above for *weighted* graphs, can be used to obtain very simple constructions of spanners with *sublinear* error terms for *unweighted* graphs. These constructions extend, improve and simplify results of Elkin, Elkin and Peleg, and Bollobás, Coppersmith and Elkin.

More specifically, we show that for any integer $k > 1$, any undirected and unweighted graph $G = (V, E)$ on n vertices has a subgraph $G' = (V, E')$ with $O(kn^{1+1/k})$ edges such that for any two vertices $u, v \in V$, if $d_G(u, v) = d$, then $d_{G'}(u, v) = d + O(d^{1-1/(k-1)})$. (Here, $d_G(u, v)$ is the distance from u to v in G.) We also show that there is a *weighted* graph $G'' = (V, E'')$ with $O(kn^{1+1/(2^{k+1}-1)})$ edges such that for every $u, v \in V$, if $d_G(u, v) = d$, then $d \leq d_{G''}(u, v) = d + O(d^{1-1/(k-1)})$. The interesting feature of these new spanners is that the *relative* error decreases with the distance.

Joint work with Mikkel Thorup.

*School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. E-mail: zwick@cs.tau.ac.il.

The walkers problem: On the cycle and the grid

J. Díaz* X. Pérez*† M.J. Serna*† N.C. Wormald†

Consider a setting in which a large number of mobile agents can perform concurrent basic movements: ahead/behind/left/right, determining a grid pattern, or left/right, describing a line. Each agent can communicate directly with any other agents which are within a given distance d. This enables communications with agents at a further distance using several intermediate agents. At each step in time there is an ad-hoc network defined by the dynamic graph whose vertex set consists of the agents, with an edge between any two agents iff they are within the distance d of each other.

Various aspects agents of such networks have been studied in the static case [AGE02, KMM99]. Algorithms for computing connectivity properties of such a network have been studied [MKPS01], and simulation results for randomly placed agents were reported there and in [HGPC99, JBAS03, RMM01], among other references. The context of these studies was a set of agents which may communicate to each other when within a given distance of each other. The networks are ad-hoc: the spatial locations of the agents determine the network. Furthermore, several of the abovementioned studies mention the dynamic situation in which the agents are mobile: connections in the network are created and destroyed as the agents move further apart or closer together. To our knowledge, ours is the first study in which the dynamic features of such a network are studied. Moreover, we obtain much sharper results on the static properties than previously obtained except for the case $d = 1$. We believe that the study of the behaviour of multiple, simultaneous random walks has its owns merits as an important open problem which could have further applications in other fields of computer science. The paper [GHSZ] also deals with the problem of maintaining connectivity of mobile agents communicating by radio frequency, but from an orthogonal prespective to the one in the present paper. It describes a *kinetic data structure* to mantain the connected components of the union of unit-radius disks moving in the plane.

We propose what we call the *walkers model*, defined as follows. A connected graph $G = (V, E)$ with $|V| = N$ is given, and a number w of *walkers* (agents). Also given is a "distance" d. A set W of walkers, with $|W| = w$, are placed randomly and independently on the vertices of G (a vertex may contain more than one walker). Each walker has a range d for communication; that is, two walkers w_1 and w_2 can communicate in one hop if the distance, in G, between the position of the walkers is at most d. Two walkers can communicate if they can reach each other by a sequence of such hops. In addition, each walker takes an independent standard random walk on G, i.e. moves at each time step to a neighbouring vertex, each neighbour chosen with equal probability.

The interesting features of the walkers model are encapsulated by the *graph of walkers*, $G_f[W]$. Here f is an a random assignment $f : W \to V$ of walkers into the vertices of G. The vertices of $G_f[W]$ are the vertices in G that contain at least one walker, two vertices in $G_f[W]$

*UPC

†Department of Combinatorics and Optimization, U. of Waterloo, Canada.

being joined by an edge iff they are at distance at most d in G. We refer to *components* of $G_f[W]$ in the usual sense, and call a component *simple* if it is formed by only one isolated vertex. We are interested in the probability of $G_f[W]$ being connected, or in the number of components and their sizes, with certain mild asymptotic restrictions on w and d.

Our primary goal with the walkers model is to characterise the dynamics of the connectivity of the network. To obtain enough information to do this, we first examine a variation of the model called the *static* model. This is a snapshot of the model at one point in time: there is merely a random assignment $f : W \to V$ of walkers into the vertices of G, and we are interested in the distribution of the number of components, as well as other information which helps to answer the dynamic questions.

In the dynamic situation, there is an initial placement of walkers as in the static case, and at each time step, every walker simultaneously moves one step to a randomly selected neighbour vertex in G. This gives rise to a random graph process, where $G_{f_t}[W]$ denotes the graph of walkers at time $t = 0, 1, \ldots$. We are interested in studying the birth and death of components, and the sudden connection and disconnection of $G_{f_t}[W]$ in a dynamic setting.

We consider a sequence of graphs G with increasing numbers of vertices N, for N tending to inifinity. The parameters w and d are functions of N. We restrict to the case $w \to \infty$ in order to avoid considering small-case effects. Of course we take $d \geq 1$. We make further restrictions on w and d in order to rule out noninteresting cases, such as values of the parameters in which the network is a.a.s. disconnected or a.a.s. connected. In this paper, we study the walkers model for two particular sequences of graphs G: the cycle of length N and the $n \times n$ toroidal grid. (In the case of the grid, we use the ℓ^p distance, for any $1 \leq p \leq \infty$.)

We study the problem for the toroidal grid T_N with $N = n^2$ nodes, where we consider any normed ℓ^p distance, for $1 \leq p \leq \infty$. Although the most interesting is the euclidian distance ℓ^p. In the static case, we sprinkle uniformly at random w walkers on T_N. We determine the connectivity treshold of the graph of walkers and the limiting distribution of the amount of components at the phase transition, in terms of N, w and d. We need to prove a *geometric lemma* bounding the size of the set of non-occupied vertices at distance at most d from the boundary of any connected component in $T_{N_f}[W]$. After, we turn to the dynamic setting where, at each time t, each walker is forced to move with probability $1/4$ to one of its neighbors, and we study the dynamic behaviour of $T_{N_{f_t}}[W]$. We provide characterisations of the probability of creation and destruction of connected components, and use it to give estimations of the expected lifespan of connected components and the expected time the graph of walkers remains connected (or disconnected).

We also will mention, similar results on other topologies, as the cycle C_N with N vertices or the hypercube H_n of dimension n.

References

[AGE02] P.K. Agarwal, L. Guibas, H. Edelsbrunner, J. Erickson, M. Isard, S. Har-Peled, J. Hershberger, C. Jensen, L. Kavraki, P. Koehl, Ming Lin, D. Manocha, D. Metaxas, B. Mirtich and D. Mount, Algorithmic issues in modeling motion. *ACM Computing Surveys*, 34:550–572, 2002.

[GHSZ] L. Guibas, J. Hershberger, S. Suri and Li Zhang, Kinetic Connectivity for Unit Disks. *Discrete and Computational Geometry*, 25:591–610, 2001.

[HGPC99] X. Hong, M. Gerla, G. Pei and C. Chiang. Group mobility model for Ad hoc wireless networks. *Proc. ACM/IEEE MSWIM*, Seattle, 1999.

[JBAS03] A. Jardosh, E. Belding-Royer, K. Almeroth and S. Suri. Towards Realisitic Mobility Models for Mobile Ad hoc Networks. *ACM Mobicom*, San Diego, 2003.

[KMM99] K. H. Kramer, N. Minar and P. Maes, Tutorial: Mobile Software Agents for Dynamic Routing. *Mobile Computing and Communications Review*, 3:12–16, 1999.

[MKPS01] S. Meguerdichian, F. Coushanfar, M. Potkonjak and M. B. Srivastava, Coverage problems in wireless ad-hoc sensor networks. *Proc. of INFOCOM*, 1380–1387, 2001.

[RMM01] E. M. Royer, P.M. Melliar-Smith and L. E. Moser, An anlysis of the optimum node density for ad hoc mobile networks *Proc. of IEEE International Conference on Communications*, 857–861, 2001.

Connectivity and information transfer in social networks

Richard Cole
New York University

Due in part to the growth of the Internet and the World Wide Web, the last 5-10 years has seen the emergence of a new style of question in computer science. There are descriptive questions; for example, what is the form of the Internet graph? There are explanatory questions; why does it work?

This genre of questions and explanations is by no means limited to the Internet. The widely known notion of "six degrees of separation" arose as a result of the following experiment. People in Nebraska were asked to mail letters to recipients in Massachusetts, by using intermediaries they knew, these intermediaries being asked to behave in the same way. Not only did a high proportion of the letters arrive, they did so by short routes of six or fewer edges. The question, of course, is why did this work? Kleinberg addressed this by demonstrating a class of augmented grid graphs which exhibited analogous behavior. Not only did his graphs have short paths between pairs of nodes, such short paths could be found by local decisions, at least with high probability. A striking feature of his routing algorithm is its simplicity.

In an analogous vein, one can ask what are the procedures that drive price adjustment in markets for goods? This was formalized long ago by economists as the problem of finding market equilibria. An early solution approach, called tatonnement, proposed the natural procedure of reducing prices of goods with insufficient demand and increasing those of goods with excess demand. Over fifty years ago, this was formalized as a differential equation, which was shown to converge to equilibrium at least when the Gross Substitutes property applied. Recently, polynomial time algorithms for finding approximate market equilibria have been found. While encouraging, these algorithms do not seem to indicate why markets might tend to be equilibrium (of course, sometimes they may not). This would appear to call for non-centralized, indeed highly distributed algorithms. Are there such algorithms?

This talk will have more questions than answers.

Approximation Algorithms for Network Problems

Susanne Albers
University of Freiburg
Germany

In this presentation we study various algorithmic problems that arise in large networks and design approximate solutions to them.

Buffer management in network switches: In the first part of the talk we investigate a basic buffer management problem. Consider a network switch with m input ports, each of which is equipped with a buffer (queue) of limited capacity. Data packets arrive online and can be stored in the buffers if space permits; otherwise packet loss occurs. In each time step the switch can transmit one packet from one of the buffers to the output port. The goal is to maximize the number of transmitted packets. We settle the competitive performance of the entire family of greedy strategies, which always serve the longest queue. We prove that greedy algorithms are not better than 2-competitive no matter how ties are broken. We then present the first deterministic online algorithm that is better than 2-competitive. We develop a modified greedy algorithm, called *Semi-Greedy*, and prove that it achieves a competitive ratio of $17/9 \approx 1.89$. Additionally we study scenarios where online algorithms are granted additional resources in terms of extra memory or higher transmission rates.

Web caching with request reorderung: In the second part of the presentation we study web caching with request reordering. The goal is to maintain a cache of web documents so that a sequence of requests can be served at low cost. To improve cache hit rates, a limited reordering of requests is allowed. We present a deterministic online algorithm that achieves an optimal competitiveness, for the most general cost model and all cache sizes. We then investigate the offline problem, which is NP-hard in general. We develop the first polynomial time algorithms that can manage arbitrary cache sizes. Our strategies achieve small constant factor approximation ratios. The algorithms are based on a general technique that reduces web caching with request reordering to a problem of computing batched service schedules.

The price of anarchy in network design: In the third part of the talk we study a network design problem in which n selfish agents have to build a network so that the resulting graph is connected. The cost of an agent consists of (a) its edge building cost and (b) its connection cost. An agent pays a non-negative cost of α for each edge it builds. The connection cost is the sum of the shortest path distances to other agents. We consider Nash equilibria for this game and analyze the price of anarchy, which is the worst-case ratio of the cost of any equilibrium to the cost of the best equilibrium. We show that, for large ranges of α, the price of anarchy is constant. We also prove that, in any case, the price of anarchy is bounded by $O(n^{1/3})$, improving the previous best bound of $O(n)$. Additionally we develop structural properties of weak Nash equilibria and study the effect of cost sharing where agent can split the cost of building edges.

Generalized linear programming

Jiří Matoušek
Charles University, Prague

Linear programming is concerned with optimizing linear functions over convex polytopes. Attempts to analyze the running time of the simplex method, as well as other motivations, have led to the notion of abstract objective functions on convex polytopes, which are linear orderings of the vertices that share some simple propeties of orderings induced by generic linear functions. Several other axiomatic frameworks generalizing linear programming have been introduced as well. In addition to linear programming they encompass many other important geometric optimization problems. Some of the algorithms for linear programming can be expressed and analyzed in these frameworks.

The talk is meant as an introduction to the concepts mentioned above, and on the more technical side, it will outline a recent result of Szabó and the speaker on bad worst-case performance of the simplex method with a certain randomized pivot rule on cubes with abstract objective functions.

My Favorite Ten Complexity Theorems of the Past Decade II

Lance Fortnow
University of Chicago

At the end of 1994 I presented my favorite ten theorems from the previous decade [1] and using them as a platform to survey the research in many areas of computational complexity during that time.

Ten years later I will present a new list of my favorite ten theorems from the decade since the original list. Once again we will use the list as a starting point to survey recent research in computational complexity. We will cover many topics including derandomization, probabilistically checkable proofs, coding theory, quantum computing and some algorithms results with complexity implications.

References

[1] L. Fortnow. My favorite ten complexity theorems of the past decade. In *Proceedings of the 14th Conference on the Foundations of Software Technology and Theoretical Computer Science*, volume 880 of *Lecture Notes in Computer Science*, pages 256–275. Springer, Berlin, 1994. Invited lecture.

Some Heuristic Analysis of Average Behavior of Local Search Algorithms

— Short Abstract —

Osamu Watanabe*
Dept. of Math. and Computing Sciences, Tokyo Institute of Technology
(watanabe@is.titech.ac.jp)

It has been known that local search algorithms (even simple ones) sometimes work reasonably well *on average* for solving NP-hard problems. Unfortunately, however, due to the difficulty of investigating the (randomized) execution of a given algorithm on random instances, our theoretical analysis on average behavior of such local search algorithms has been limited. For obtaining better understanding of local search algorithms and their average behavior, we proposed [1] the following *heuristic approach*: First consider some relatively simple Markov process simulating algorithm's execution, and then analyze this simple Markov process.

In this talk, we consider the following variation of 3SAT problem.

3-CNF-SAT (from some nice initial assignment)

Input. A 3-CNF formula F on n variables and an initial assignment $\boldsymbol{a}$.
Task. Find a sat. assignment for F.
Promise. F is satisfiable with some sat. assignment whose Ham. distance from $\boldsymbol{a}$ is pn for some $p > 0$.

We also consider 3-$\oplus$-SAT, which is defined in the same way except that each clause of F consisits of the parity of three literals.

For these problems, we analyze variations of local search algorithms by our approach, and discuss how small algorithmic changes affect their average performance.

[1] O. Watanabe, T. Sawai, and H. Takahashi, Analysis of a randomized local search algorithm for LDPCC decoding problem, in *Proc. SAGA'03*, Lecture Notes in Comp. Sci. 2827,50–60, 2003.

*Supported in part by a Grant-in-Aid for Scientific Research on Priority Areas "Statical-Mechanical Approach to Probabilistic Information Processing" 2002-2005.

Table of Contents

Fast and Sensitive Homology Search
Ming Li 398

Dynamic Graph Algorithms with Applications
Mikkel Thorup 405

Approximation Algorithms for Stochastic Combinatorial Optimization
R. Ravi 410

More Approximation Algorithms for Stochastic Programming Problems
David Shmoys 432

Efficient Haplotype Inference on Pedigrees and Applications in Gene Association Mapping
Tao Jiang 440

New Horizons in Machine Learning
Avrim Blum 448

Rigorous Analysis of Heuristics for NP-hard Problems
Uriel Feige 454

Data Stream Algorithms in Computational Geometry
Timothy M. Chan 462

Steps into Computational Algebraic Topology
Herbert Edelsbrunner 471

Efficient Algorithms for the Longest Path Problem
Ryuhei Uehara 475

Proposal of Asynchronous Distributed Branch and Bound
Shigeru Masuyama 481

Energy-Optimal Online Algorithms for Broadcasting in Wireless Networks
Hirotaka Ono 487

Ultimate Implementation and Analysis of the AMO Algorithm for Pricing European-Asian Options
Akiyoshi Shioura 492

On Computing all Abductive Explanations from a Propositional Horn Theory
Kazuhisa Makino 495

Metric Labeling: Upper and Lower Bounds
Seffi Naor 504

Approximate Distance Oracles and Spanners with Sublinear Error Terms
Uri Zwick 518

The Walkers Problem: On the Cycle and the Grid
Josep Diaz 523

Approximation Algorithms for Network Problems
Susanne Albers 537

Generalized Linear Programming
Jiří Matoušek 546

My Favorite Ten Complexity Theorems of the Past Decade II
Lance Fortnow 552

Some Heuristic Analysis of Average Behavior of Local Search Algorithms
Osamu Watanabe 561

Faster and More Sensitive Homology Search

Ming Li
Visiting Professor
City University of Hong Kong

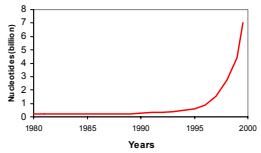
Canada Research Chair in Bioinformatics
Professor
University of Waterloo

Joint work with Bin Ma, John Tromp

I will present one simple idea
which is directly benefiting thousands of people daily

A gigantic gold mine

- The trend of genetic data growth



30 billion
in year 2005

- 400 Eukaryote genome projects underway
- GenBank doubles every 18 months
- Comparative genomics all-against-all search

Comparing to internet search

- Internet search
  - Size limit: 5 billion people x homepage size
  - Supercomputing power used: ½ million CPU-hours/day
  - Query frequency: Google --- 112 million/day
  - Query type: exact keyword search --- easy to do
- Homology search
  - Size limit: 5 billion people x 3 billion basepairs + millions of species x billion bases
  - 10% (?) of world's supercomputing power
  - Query frequency: NCBI BLAST -- 150,000/day, 15% increase/month
  - Query type: approximate search --- topics today

Tremendous Cost

- Bioinformatics Companies living on BLAST:
  - Paracel (Celera)
  - TimeLogic
  - TurboGenomics (TurboWorx)
- NSF, NIH, pharmaceuticals *proudly* support many supercomputing centers for homology search
- However: hardware become obsolete in 2-3 years. Software solution is indispensable.

Outline

- **What is homology search**
- A simple (but profound) idea
- Its theory
- Its practical success

What is homology search

- Given two DNA sequences, find all local similar regions, using "edit distance" (match=1, mismatch=-1, gapopen=-5, gapext=-1).
- Example. Input:
  - E. coli genome: 5 million base pairs
  - H. influenza genome: 1.8 million base pairs

  Output: all local alignments.

Time Flies

- Dynamic programming (1970-1980)
  - Human vs mouse genomes: 10^4 CPU-years
- BLAST, FASTA heuristics (1980-1990)
  - Human vs mouse genomes: 19 CPU-years
  - BLAST paper was referenced 100000 times
- PatternHunter
  - Human vs mouse genomes: 20 CPU-days

Outline

- What is homology search
- **A simple (but profound) idea**
- Its theory
- Its practical success

BLAST Algorithm & Example

- Find seeded matches of 11 base pairs
- Extend each match to right and left, until the scores drop too much, to form an alignment
- Report all local alignments

Example:

```
0001110111111111100110111 0
AGCGATGTCAGGCGCCCGTATTTCCGTA
   |||  |||x|||||||   ||  ||||
TCGGATCTCACGCGCCCGGCTTACCGTG
```

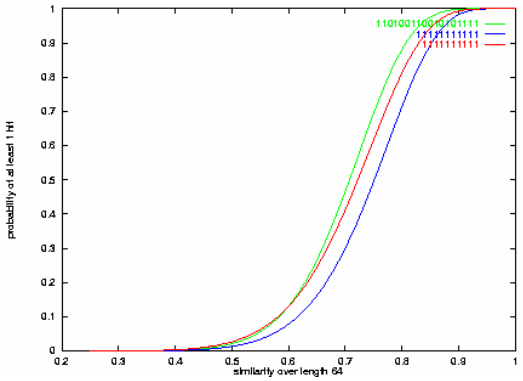
BLAST Dilemma:

- If you want to speed up, have to use a longer seed. However, we now face a dilemma:
  - increasing seed size speeds up, but loses sensitivity;
  - decreasing seed size gains sensitivity, but loses speed.
- How do we increase sensitivity & speed simultaneously? For 20 years, many tried: suffix tree, better programming ..

New Idea: Spaced Seed

- Spaced Seed: nonconsecutive matches and optimize match positions.
- Represent BLAST seed by 11111111111
- Spaced seed: 111*1**1*1**11*111
  - 1 means a required match
  - * means "don't care" position
- This seemingly simple change makes a huge difference: significantly increases hit to homologous region while reducing bad hits.

Sensitivity: PH weight 11 seed vs BLAST 11 & 10



Outline

- What is homology search
- A simple (but profound) idea
- **Its theory**
- Its practical success

Formalize

- Given i.i.d. sequence (homology region) with Pr(1)=p and Pr(0)=1-p for each bit:

```
1100111011101101011101101011111011101
                111*1**1*1**11*111
```

- Which seed is more likely to hit this region:
  - BLAST seed: 11111111111
  - Spaced seed: 111*1**1*1**11*111

Expect Less, Get More

- Lemma: The expected number of hits of a weight W length M seed model within a length L region with homology level p is
  $(L-M+1)p^W$
  Proof. $E(\#hits) = \Sigma_{i=1 \ldots L-M+1} p^W$ ■
- Example: In a region of length 64 with p=0.7
  - Pr(BLAST seed hits)=0.3
    E(# of hits by BLAST seed)=1.07
  - Pr(optimal spaced seed hits)=0.466, 50% more
    E(# of hits by spaced seed)=0.93, 14% less

Why Is Spaced Seed Better?

A wrong, but intuitive, proof: seed s, interval I, similarity p

$E(\#hits) = Pr(s\ hits)\ E(\#hits \mid s\ hits)$

Thus:

$Pr(s\ hits) = Lp^w / E(\#hits \mid s\ hits)$

For optimized spaced seed, E(#hits | s hits)

111*1**1*1**11*111	Non overlap	Prob
111*1**1*1**11*111	6	p^6
111*1**1*1**11*111	6	p^6
111*1**1*1**11*111	6	p^6
111*1**1*1**11*111	7	p^7
.....		

- For spaced seed: the divisor is $1+p^6+p^6+p^6+p^7+ \ldots$
- For BLAST seed: the divisor is bigger: $1+ p + p^2 + p^3 + \ldots$

Complexity of finding the optimal spaced seed (Li, Ma, manuscript)

Theorem 1. Given a seed and it is NP-hard to find its sensitivity, even in a uniform region.

Theorem 2. The sensitivity of a given seed can be efficiently approximated with arbitrary accuracy, with high probability.

Theorem 3. Optimal seeds can be found in exponential time deterministically. Near optimal seed can be found in $O(n^{\log n})$ time probabilistically.

Computing Spaced Seeds

(Keich, Li, Ma, Tromp, *Discrete Appl. Math*)

Let $f(i,b)$ be the probability that seed s hits the length i prefix of R that ends with b.

Thus, if s matches b, then

$$f(i,b) = 1,$$

otherwise we have the recursive relationship:

$$f(i,b) = (1-p)f(i-1,0b') + pf(i-1,1b')$$

where b' is b deleting the last bit.

Then the probability of s hitting R is

$$\Sigma_{|b|=M}\ Prob(b)\ f(L-M,b)$$

Prior Literature

- Random or multiple spaced q-grams were used in the following work:
  - FLASH by Califano & Rigoutsos
  - Multiple filtration by Pevzner & Waterman
  - LSH of Buhler
  - Praparata et al

Outline

- What is homology search
- A simple (but profound) idea
- Its theory
- **Its practical success**

PatternHunter

(Ma, Tromp, Li: *Bioinformatics*, 18:3, 2002, 440-445)

- PH used optimal spaced seeds, novel usage of data structures: red-black tree, queues, stacks, hashtables, new gapped alignment algorithm.
- Written in Java.
- Used in Mouse Genome Consortium (*Nature*, Dec. 5, 2002), as well as in hundreds of institutions and industry.

Comparison with BLAST

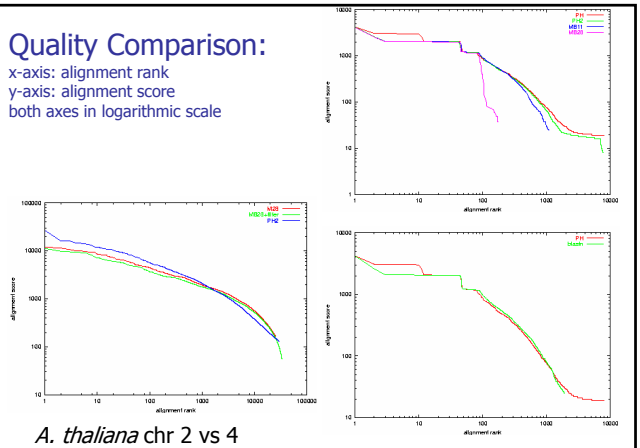
- On Pentium III 700MH, 1GB

	BLAST	PatternHunter
E.coli vs H.inf	*716s*	*14s/68M*
Arabidopsis 2 vs 4	--	*498s/280M*
Human 21 vs 22	--	*5250s/417M*
Human(3G) vs Mouse(x3=9G)*	*19 years*	*20 days*

- All with filter off and identical parameters
- 16M reads of Mouse genome against Human genome for MIT Whitehead. Best BLAST program takes 19 years at the same sensitivity

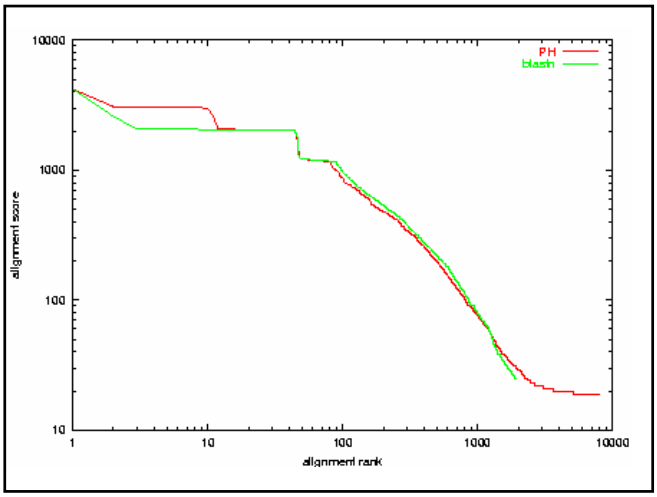
Quality Comparison:

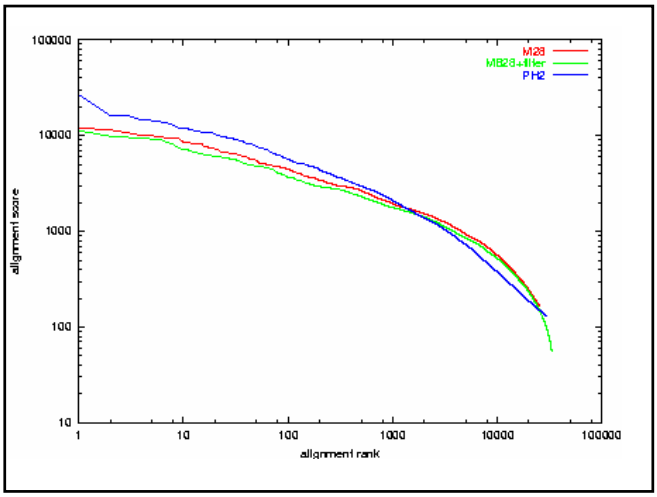
x-axis: alignment rank
y-axis: alignment score
both axes in logarithmic scale



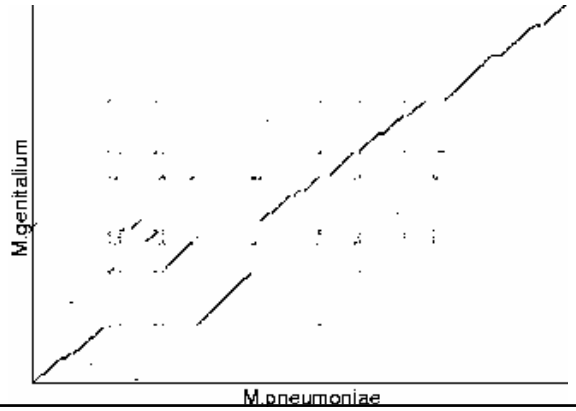
A. thaliana chr 2 vs 4

E. Coli vs *H. influenza*





Genome Alignment by PatternHunter (4 seconds)



PattternHunter II:

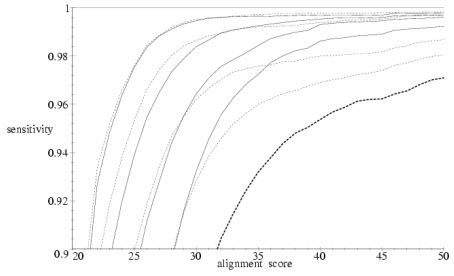
-- Smith-Waterman Sensitivity, BLAST Speed

(Li, Ma, Kisman, Tromp, *J. Bioinfo Comput. Biol.* 2004)

- The biggest problem for BLAST was low sensitivity (and low speed). Massive parallel machines are built to do S-W exhaustive dynamic programming.
- Spaced seeds give PH a *unique* opportunity of using several optimal seeds to achieve optimal sensitivity, this was not possible by BLAST technology.
- We have designed PH II, with multiple optimal seeds.
- PH II approaches Smith-Waterman sensitivity, and 3000 times faster.
- Experiment: 29715 mouse EST, 4407 human EST.

Sensitivity Comparison with Smith-Waterman (at 100%)

The thick dashed curve is the sensitivity of BLAST, seed weight 11. From low to high, the solid curves are the sensitivity of PH II using 1, 2, 4, 8 weight 11 coding region seeds, and the thin dashed curves are the sensitivity 1, 2, 4, 8 weight 11 general purpose seeds, respectively



Speed Comparison with Smith-Waterman

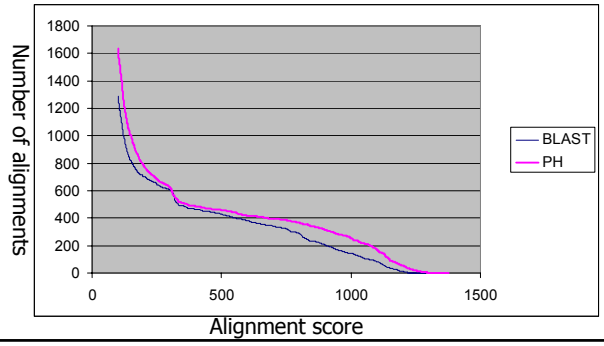
- Smith-Waterman (SSearch): 20 CPU-days.
- PatternHunter II with 4 seeds: 475 CPU-seconds. 3638 times faster than Smith-Waterman dynamic programming at the same sensitivity.

Translated PatternHunter

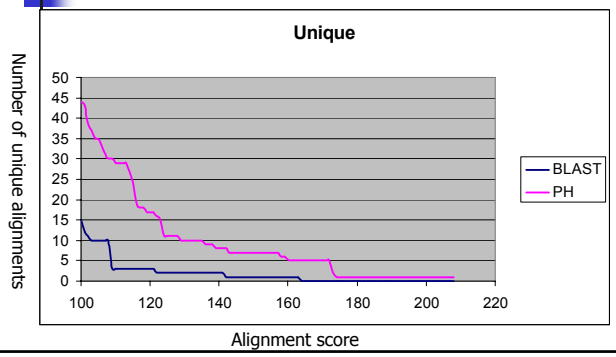
- Has all the functionalities of
  - Blastp
  - tBlastx – with gapped alignments
  - tBlastn, Blastx – with gapped alignments
- More sensitive and faster – new algorithm replacing 6-frame translation

Alignment comparison: tBLASTx vs tPH

tPH: 253 seconds
tBLASTx: 807 seconds



Unique Alignments: tBLASTx vs tPH



Old field, new trend

- Research trend
  - Over 30 papers on spaced seeds have appeared since our original paper, in 2 years.
  - Many more have used PH in their work.
  - Most modern alignment programs (including BLAST) have now adopted spaced seeds
  - Spaced seeds are serving thousands of users/day
- PatternHunter direct users
  - Pharmaceutical/biotech firms.
  - Mouse Genome Consortium, *Nature, Dec. 5, 2002.*
  - Hundreds of academic institutions.

Running PH

Available at: www.BioinformaticsSolutions.com

Java –Xmx512m –jar ph.jar –i query.fna –j subject.fna –o out.txt

-Xmx512m --- for large files
-j missing: query.fna self-comparison
-db: multiple sequence input, 0,1,2,3 (no, query, subject, both)
-W: seed weight
-G: open gap penalty (default 5)
-E: gap extension (default 1)
-q: mismatch penalty (default 1)
-r: reward for match (default 1)
-model: specify model in binary
-H: hits before extension
-P: show progress
-multi 4: use 4 seeds

Conclusion

Best ideas are simple ones. I hope I have presented one such idea today.

Open questions:

- Polynomial time probabilistic algorithm for finding (near) optimal seed, multiple seeds.
- Tighter bounds on why spaced seeds are better.
- Applications to other areas.

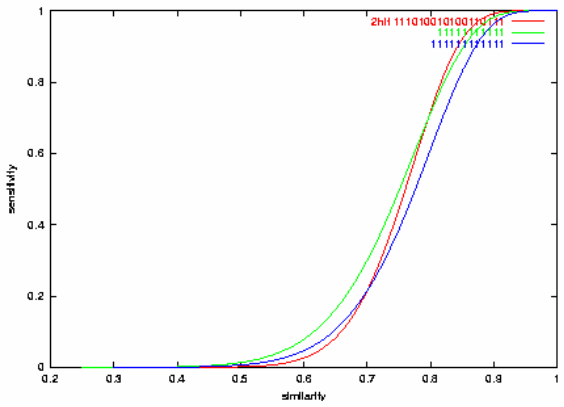
Acknowledgement

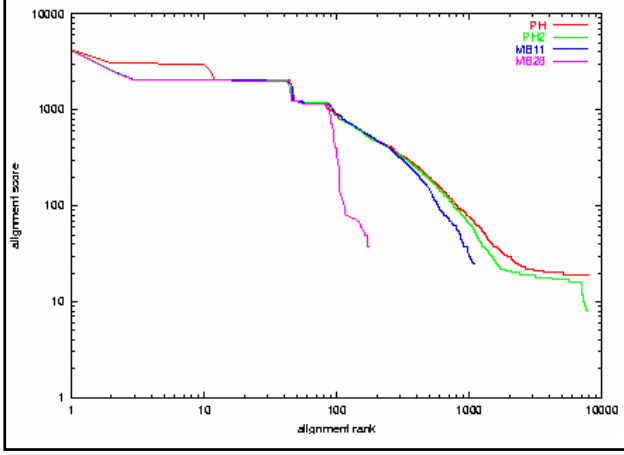
- PH is joint work with Bin Ma and John Tromp
- PH II is joint work with Ma, Kisman, and Tromp
- Some joint theoretical work with Ma, Keich, Tromp, Xu, and Brown.
- Financial support: Bioinformatics Solutions Inc, NSERC, Killam Fellowship, Steacie Fellowship, CRC chair program.

Conclusion – continued

- Another simple idea applied to data mining: from irreversibly computing 1 bit requires 1kT energy (von Neumann, Landauer), we derived shared information d(x,y) between x,y, to classify
  - Species & genomes, Li *et al*, in *Bioinformatics*, 2001
  - Chain letters, Bennett, Li, Ma, *Scientific American*, 2003
  - Languages, Benedeto,Caglioti,Loreto, *Phy. Rev. Let.*'02
  - Music, Cilibrasi, Vitanyi, de Wolf, *New Scientist*, 2003
  - Time series/anomaly detection, Keogh, Lonardi, Ratanamahatana, KDD'04. They compared d(x,y) with 51 methods/measures from SIGKDD, SIGMOD, ICDM, ICDE, SSDB, VLDB, PKDD, PAKDD and concluded our method the simplest & best --- Keogh tutorial ICDM'04.

PH 2-hit sensitivity vs BLAST 11, 12 1-hit





Natura enim simplex est,
et rerum causis superfluis non luxuriat.
I. Newton

Dynamic graph algorithms with applications

Mikkel Thorup
AT&T Labs–Research

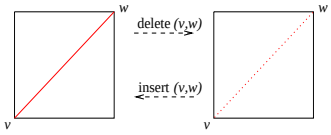
Dynamic data structures in static problems

Standard example: priority queue in greedy algorithm such as Dijkstra's single source shortest path algorithm.

Here we consider dynamic graph algorithms maintaining properties and objects in a changing graph.

Dynamic graph algorithms

Updates



Connectivity — disconnected? — connected *(v,w)*

2-edge-connectivity — bridge? — 2-edge-connected *(v,w)*

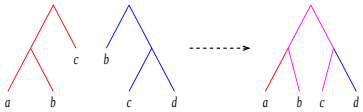
Biconnectivity — articulatiion point? — biconnectied *(v,w)*

Minimum spanning tree (MST)

Update MST during insertion and deletion

Applications

- Constructing tree from homeomorphic subtrees



- Unique perfect matching

We shall also talk about dynamic shortest paths and their applications.

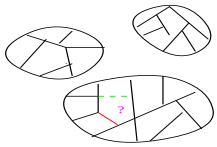
Connectivity of $G = (V, E)$, $|V| = n$, during m updates, starting $E = \emptyset$.

Maintain spanning forest F

(for dynamic forest F "everything" takes $O(\log n)$ time)

insert$((v, w))$ if v and w disconnected in F, $F := F \cup \{(v, w)\}$

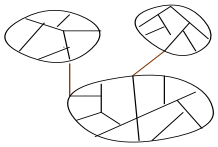
delete$((v, w))$ if $(v, w) \in F$, seek replacement edge from E reconnecting $F \setminus \{(v, w)\}$



Introduce levels $\ell : E \to \{0, ..., \lfloor \log_2 n \rfloor\}$

$G_i = (V, \{e \in E : \ell(e) \geq i\})$

(i) F ℓ-maximal spanning forest
$\Rightarrow F_i = F \cap G_i$ spanning forest of G_i



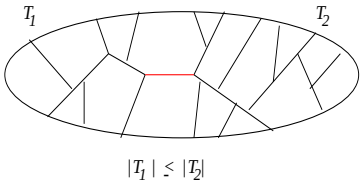
(ii) Components of G_i contain $\leq n/2^i$ vertices.

Idea: amortize over level increases

Insert$((v, w))$: $\ell((v, w)) := 0$.
If v and w disconnected in F, $F \cup \{(v, w)\}$

Delete(e): If $e \in F$, $F := (F \setminus \{e\}) \cup$ Replace(e)

Replace(e)
For $i := \ell(e)$ downto 0 do
▷ no replacement edge on level $> i$



▷ level i replacement connect T_1 and T_2
▷ $|T_1| \leq n/2^{i+1}$
For all level i edges $f \in T_1$: $\ell(f) := i+1$.
Consider level i edges (v, w), $v \in T_1$, one by one:
If $w \notin T_1$, return $\{(v, w)\}$.
Else $\ell((v, w)) := i + 1$.
Return $\emptyset$

Each statement iterated $\leq m \log_2 n$ times
$\wedge$ each statement supported in $O(\log n)$ time
$\Rightarrow O(m \log^2 n)$ total time.

Decremental MST of $G = (V, E)$, $|V| = n$, $|E| = m$.

Maintain minimum spanning forest F

delete$((v, w))$ if $(v, w) \in F$, seek lightest replacement from E reconnecting $F \setminus \{(v, w)\}$

Introduce levels $\ell : E \to \{0, ..., \lfloor \log_2 n \rfloor\}$

$G_i = (V, \{e \in E : \ell(e) \geq i\})$

(i) F ℓ-maximal spanning forest
$\Rightarrow F_i = F \cap G_i$ spanning forest of G_i

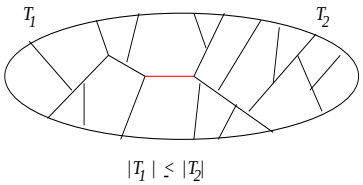
(ii) Components of G_i contain $\leq n/2^i$ vertices.

Initially F minimum spanning forest
and $\forall e \in E : \ell(e) = 0$

Delete(e): if $e \in F$, $F := (F \setminus \{e\}) \cup$ Replace(e)

Replace(e)

For $i := \ell(e)$ downto 0 do

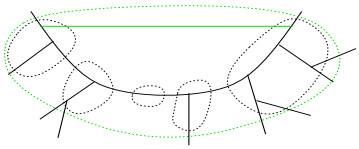


For all level i edges $f \in T_1$: $\ell(f) := i+1$.
Consider level i edges (v, w), $v \in T_1$, one by one, in order of increasing weight:
If $w \notin T_1$, return $\{(v, w)\}$.
Else $\ell((v, w)) := i + 1$.
Return $\emptyset$

→ fully-dynamic polylogarimic MST using general reduction of Henzinger and King (ICALP'97).

2-edge-connectivity of $G = (V, E)$, $|V| = n$, during m updates, starting with $E = \emptyset$.

Maintain spanning forest F



$(v, w) \in E$ covers path $v \cdots w$ from v to w in F

Lem x and y 2-edge connected $\iff$ $x \cdots y$ covered.

Introduce levels $\ell : E \setminus F \to \{0, ..., \lfloor \log_2 n \rfloor\}$

$G_i = (V, F \cup \{e \in E : \ell(e) \geq i\})$

(i) 2-edge connected components of G_i contain $\leq n/2^i$ vertices.

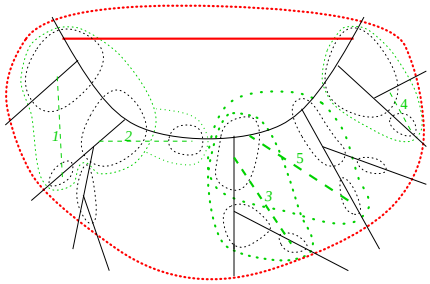
For each $f \in F$ maintain highest level of covering edge, denoted $c(f)$. If f bridge, $c(f) = -1$.

Connected(x, y): $\forall e \in x \cdots y : c(e) \geq 0$.

Insert$((v, w))$
If v and w disconnected in F,
$F \cup \{(v, w)\}$.
$c((v, w)) := -1$.
Else
$\ell((v, w)) := 0$
call Cover$\ell((v, w))$

Cover$((v, w))$
For all $f \in v \cdots w$ with $c(f) < \ell((v, w))$,
$c(f) := (v, w)$.

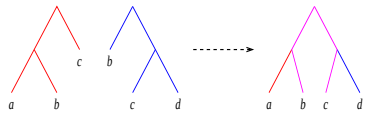
Delete(e)
if $e \in F$,
swap e in F with covering edge f on highest level
$(c(f), \ell(e)) := (\ell(f), c(e))$
$e := f$
Recover(e)



Cover only called $O(m \log n)$ times, each at polylogarithmic cost using data structures for dynamic forests.

Applications

Constructing tree from homeomorphic subtrees



Reduction to decremental connectivity by Henzinger, King, and Warnow (SODA'96)

Small trees represented as triples $((a,b),c) \in T$ with $a,b,c \in A$.

Obs If $((a,b),c) \in T$, a and b must descend from same child of root.

Make child for each component of $G = (A, \{(a,b) : ((a,b),c) \in T\})$

This resolves all triples $((a,b),c)$ with c disconnected from b (and a) in G.

Grandchildren found by removing edge (a,b) for each resolved triple $((a,b),c)$.

Unique perfect matchings

Reduction to decremental 2-edge connectivity by Gabow, Kaplan, and Tarjan (STOC'99)

Lem (Kotzig 1959) A unique perfect matching has a bridge.

Constructing unique perfect matching, if any

$M := \emptyset$
While component C of G has bridge (v,w)
  If components of $C \setminus \{(v,w)\}$ both have odd number of vertices,
    $M := M \cup \{(v,w)\}$.
    Delete all edges incident to v and w from G.
  Elseif components of $C \setminus \{(v,w)\}$ both have even number of vertices,
    Delete (v,w) from G.
  Else G has no perfect matching. EXIT.
If G empty, return M;
Else G has no perfect matching.

...another application

Thm (Petersen 1891) Every bridgeless 3-regular graph has a perfect matching.

Biedl, Bose, Demaine, and Lubiw (SODA'99) have used dynamic 2-edge connectivity to construct such a perfect matching in $\tilde{O}(n)$ time, improving over the bound the $\tilde{O}(n^{3/2})$ obtained using the general time bound for matching when $m = O(n)$.

Shortest paths: some techniques

Ramalingam and Reps suggested lazy Dijkstra for single source shortest paths.

- Running time proportional to # edges incident to vertices changing distance from source.
- Works great in practice.

Recent break-through by Demetrescu and Italiano on all pairs-shortest path:

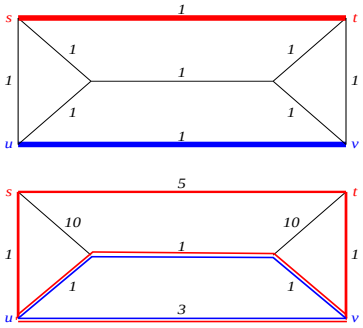
- Each vertex update supported in $\tilde{O}(n^2)$ time.
- Works even better in practice.
- Current best has update time $O(n^2(\log n + \log^2(m/n))$ and works for arbitrary weights [Thorup].

Internet traffic engineering

Demand of 1 for (s,t) and (u,v)

General routing: max load 2/3

Shortest path routing: max load 1 or 3/4



Optimizing shortest path routing with dynamic shortest paths [Fortz Thorup]

Finding weights minimizing max utilization (load/capacity) within factor 3/2 is NP-hard.

Cisco default: link weight inverse of capacity.

Local search heuristics

Iteratively change a weight that reduces max-utilization.

When inner loop tries a weight change, new shortest path routes are found and evaluated.

Ramalingam and Reps gave speed-up by factor 15 with 100 nodes and 300 edges.

Gained 50% over Cisco default on AT&T IP backbone.

Got within few percent of optimal general routing.

Concluding remarks

Talked about dynamic graph algorithms and their applications in solving static problems

Similar to priority queues in greedy algorithms

Challenge: dynamic reachability between fixed s and t for sparse graphs
$\rightarrow$ better augmenting paths max-flow algorithms.

Approximation Algorithms for Stochastic Combinatorial Optimization

R. Ravi
Carnegie Mellon University

Joint work with:
Kedar Dhamdhere, CMU
Anupam Gupta, CMU
Martin Pal, DIMACS
Mohit Singh, CMU
Amitabh Sinha, U. Michigan

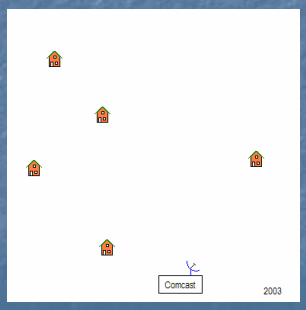
Sources: [RS IPCO 04, GPRS STOC 04, GRS FOCS 04, DRS IPCO 05]

Outline

- Motivation: The cable company problem
- Model and literature review
- Solution to the cable company problem
- General covering problem
- Scenario dependent cost model

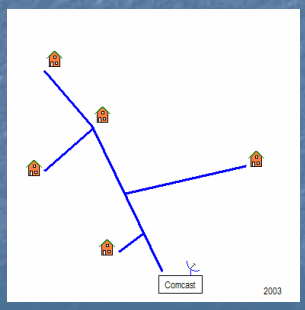
The cable company problem

- Cable company plans to enter a new area
- Currently, low population
- Wants to install cable infrastructure in anticipation of future demand



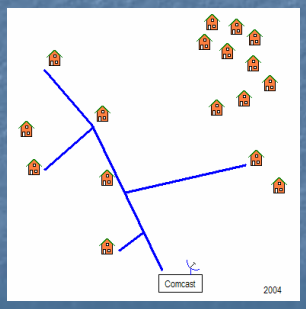
The cable company problem

- Future demand unknown, yet cable company needs to build now
- Where should cable company install cables?



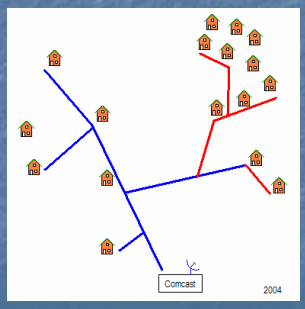
The cable company problem

- Future demand unknown, yet cable company needs to build now
- Where should cable company install cables?



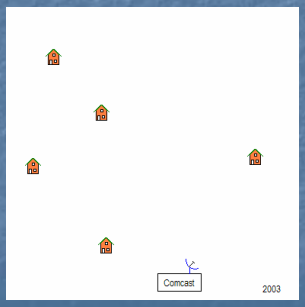
The cable company problem

- Future demand unknown, yet cable company needs to build now
- Where should cable company install cables?



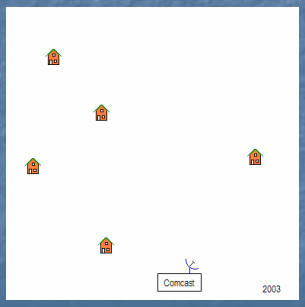
The cable company problem

- Future demand unknown, yet cable company needs to build now
- Where should cable company install cables?



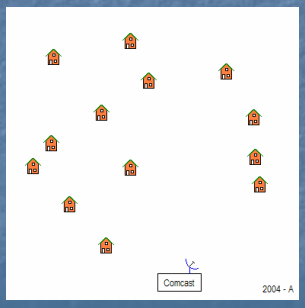
The cable company problem

- Future demand unknown, yet cable company needs to build now
- Forecasts of possible future demands exist
- Where should cable company install cables?



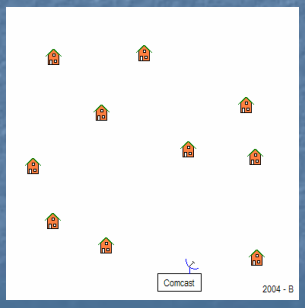
The cable company problem

- Future demand unknown, yet cable company needs to build now
- Forecasts of possible future demands exist
- Where should cable company install cables?



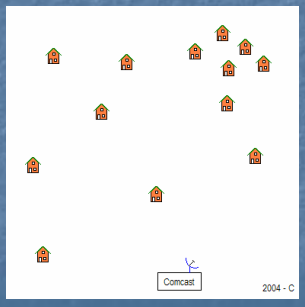
The cable company problem

- Future demand unknown, yet cable company needs to build now
- Forecasts of possible future demands exist
- Where should cable company install cables?



The cable company problem

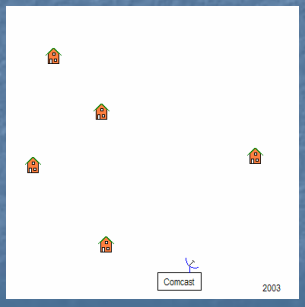
- Future demand unknown, yet cable company needs to build now
- Forecasts of possible future demands exist
- Where should cable company install cables?



The cable company problem

- cable company wants to use demand forecasts, to

Minimize
Today's install. costs
+ Expected future costs



Outline

- Motivation: The cable company problem
- Model and literature review
- Solution to the cable company problem
- General covering problem
- Scenario dependent cost model

Stochastic optimization

- Classical optimization assumed deterministic inputs

Stochastic optimization

- Classical optimization assumed deterministic inputs
- Need for modeling data uncertainty quickly realized [Dantzig '55, Beale '61]

Stochastic optimization

- Classical optimization assumes deterministic inputs
- Need for modeling data uncertainty quickly realized [Dantzig '55, Beale '61]
- [Birge, Louveaux '97, Klein Haneveld, van der Vlerk '99]

Model

Two-stage stochastic opt. with recourse

Model

Two-stage stochastic opt. with recourse

- Two stages of decision making, with limited information in first stage

Model

Two-stage stochastic opt. with recourse

- Two stages of decision making
- Probability distribution governing second-stage data and costs given in 1st stage

Model

Two-stage stochastic opt. with recourse

- Two stages of decision making
- Probability dist. governing data and costs
- Solution can always be made feasible in second stage

Mathematical model

- Ω: probability space of 2nd stage data

$$\begin{array}{lllll} \min & c.x & + E[c(\omega)y(\omega)] & & \\ & A.x & & \leq & b \\ & T(\omega).x & + W(\omega).y(\omega) & \leq & h(\omega) \quad \forall \omega \in \Omega \\ & x \in P, & y(\omega) \in P(\omega) & & \end{array}$$

Mathematical model

- Ω: probability space of 2nd stage data

$$\begin{array}{lllll} \min & c.x & + E[c(\omega)y(\omega)] & & \\ & A.x & & \leq & b \\ & T(\omega).x & + W(\omega).y(\omega) & \leq & h(\omega) \quad \forall \omega \in \Omega \\ & x \in P, & y(\omega) \in P(\omega) & & \end{array}$$

- Extensive form: Enumerate over all $\omega \in \Omega$

Scenario models

- Enumerating over all $\omega \in \Omega$ may lead to very large problem size
- Enumeration (or even approximation) may not be possible for continuous domains

New model: Sampling Access

- "Black box" available which generates a sample of 2nd stage data with same distribution as actual 2nd stage
- Bare minimum requirement on model of stochastic process

Computational complexity

- Stochastic optimization problems solved using Mixed Integer Program formulations
- Solution times prohibitive
- NP-hardness inherent to problem, not formulation: E.g., 2-stage stochastic versions of MST, Shortest paths are NP-hard.

Our goal

- Approximation algorithm using sampling access
  - cable company problem
  - General model – extensions to other problems

Our goal

- Approximation algorithm using sampling access
  - cable company problem
  - (General model – extensions to other problems)
- Consequences
  - Provable guarantees on solution quality
  - Minimal requirements of stochastic process

Previous work

- Scheduling with stochastic data
  - Substantial work on exact algorithms [Pinedo '95]
  - Some recent approximation algorithms [Goel, Indyk '99; Möhring, Schulz, Uetz '99]
- Approximation algorithms for stochastic models
  - Resource provisioning with polynomial scenarios [Dye, Stougie, Tomasgard Nav. Res. Qtrly '03]
  - "Maybecast" Steiner tree: $O(\log n)$ approximation when terminals activate independently [Immorlica, Karger, Minkoff, Mirrokni '04]

Our work

- Approximation algorithms for two-stage stochastic combinatorial optimization
  - Polynomial Scenarios model, several problems using LP rounding, incl. Vertex Cover, Facility Location, Shortest paths [R., Sinha, July '03, appeared IPCO '04]
  - Black-box model: Boosted sampling algorithm for covering problems with subadditivity – general approximation algorithm [Gupta, Pal, R., Sinha STOC '04]
  - Steiner trees and network design problems: Polynomial scenarios model, Combination of LP rounding and Primal-Dual [Gupta, R., Sinha FOCS '04]
  - Stochastic MSTs under scenario model and Black-box model with polynomially bounded cost inflations [Dhamdhere, R., Singh, To appear, IPCO '05]

Related work

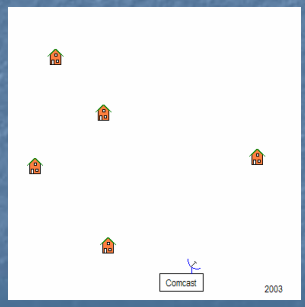
- Approximation algorithms for Stochastic Combinatorial Problems
  - Vertex cover and Steiner trees in restricted models studied by [Immorlica, Karger, Minkoff, Mirrokni SODA '04]
  - Rounding for stochastic Set Cover, FPRAS for #P hard Stochastic Set Cover LPs [Shmoys, Swamy FOCS '04]
  - Multi-stage stochastic Steiner trees [Hayrapetyan, Swamy, Tardos SODA '05]
  - Multi-stage Stochastic Set Cover [Shmoys, Swamy, manuscript '04]
  - Multi-stage black box model – Extension of Boosted sampling with rejection [Gupta, Pal, R., Sinha manuscript '05]

Outline

- Motivation: The cable company problem
- Model and literature review
- Solution to the cable company problem
- General covering problem
- Scenario dependent cost model

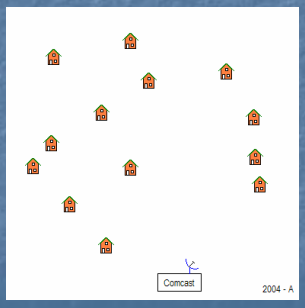
The cable company problem

- Cable company wants to install cables to serve future demand



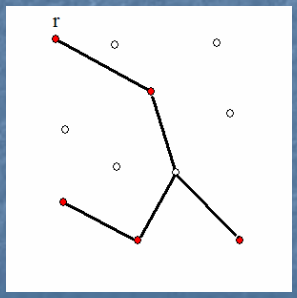
The cable company problem

- Cable company wants to install cables to serve future demand
- Future demand stochastic, cables get expensive next year
- What cables to install this year?



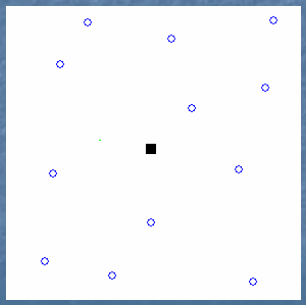
Steiner Tree - Background

- Graph $G=(V,E,c)$
- Terminals S, root $r \in S$
- Steiner tree: Min cost tree spanning S
- NP-hard, MST is a 2-approx, Current best 1.55-approx (Robins, Zelikovsky '99)
- Primal-dual 2-approx (Agrawal, Klein, R. '91; Goemans, Williamson '92)



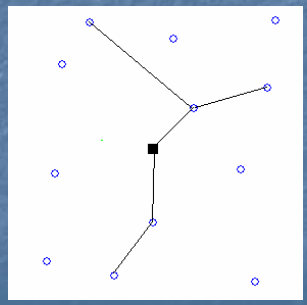
Stochastic Min. Steiner Tree

- Given a metric space of points, distances c_e
- Points: possible locations of future demand
- Wlog, simplifying assumption: no 1st stage demand



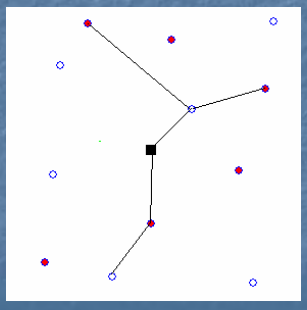
Stochastic Min. Steiner Tree

- Given a metric space of points, distances c_e
- 1st stage: buy edges at costs c_e



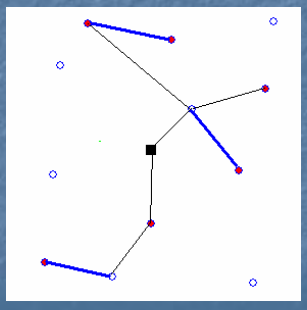
Stochastic Min. Steiner Tree

- Given a metric space of points, distances c_e
- 1st stage: buy edges at costs c_e
- 2nd stage: Some clients "realized", buy edges at cost $\sigma.c_e$ to serve them ($\sigma > 1$)



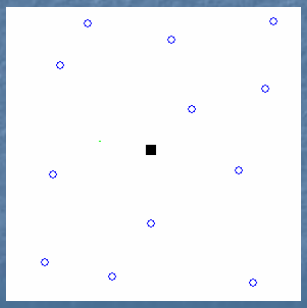
Stochastic Min. Steiner Tree

- Given a metric space of points, distances c_e
- 1st stage: buy edges at costs c_e
- 2nd stage: Some clients "realized", buy edges at cost $\sigma.c_e$ to serve them ($\sigma > 1$)



Stochastic Min. Steiner Tree

- Given a metric space of points, distances c_e
- 1st stage: buy edges at costs c_e
- 2nd stage: Some clients "realized", buy edges at cost $\sigma.c_e$ to serve them ($\sigma > 1$)
- Minimize exp. cost



Algorithm Boosted-Sample

- Sample from the distribution of clients σ times (sampled set S)

Algorithm Boosted-Sample

- Sample from the distribution of clients σ times (sampled set S)
- Build minimum spanning tree T_0 on S
  - Recall: Minimum spanning tree is a 2-approximation to Minimum Steiner tree

Algorithm Boosted-Sample

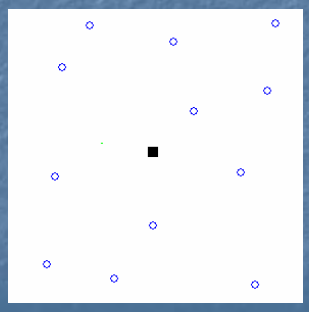
- Sample from the distribution of clients σ times (sampled set S)
- Build minimum spanning tree T_0 on S
- 2nd stage: actual client set realized (R)
  - Extend T_0 to span R

Algorithm Boosted-Sample

- Sample from the distribution of clients σ times (sampled set S)
- Build minimum spanning tree T_0 on S
- 2nd stage: actual client set realized (R)
  - Extend T_0 to span R
- Theorem: 4-approximation!

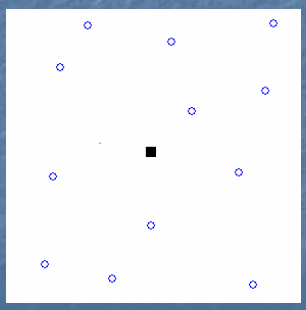
Algorithm: Illustration

- Input, with $\sigma=3$



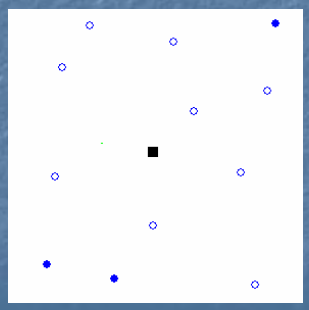
Algorithm: Illustration

- Input, with $\sigma=3$
- Sample σ times from client distribution



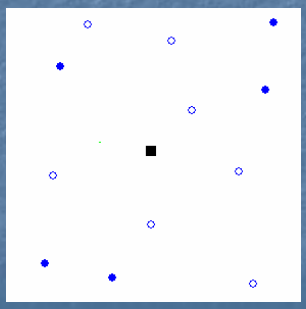
Algorithm: Illustration

- Input, with $\sigma=3$
- Sample σ times from client distribution



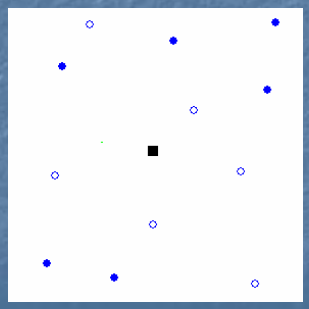
Algorithm: Illustration

- Input, with $\sigma=3$
- Sample σ times from client distribution



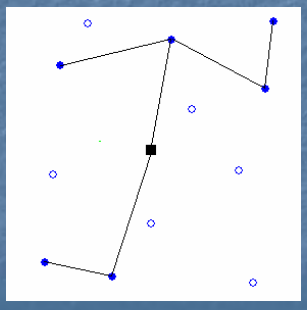
Algorithm: Illustration

- Input, with $\sigma=3$
- Sample σ times from client distribution



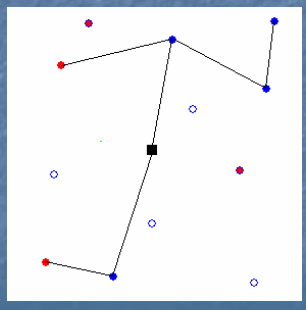
Algorithm: Illustration

- Input, with $\sigma=3$
- Sample σ times from client distribution
- Build MST T_0 on S



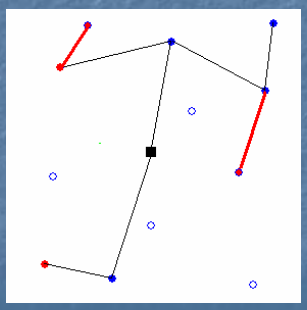
Algorithm: Illustration

- Input, with $\sigma=3$
- Sample σ times from client distribution
- Build MST T_0 on S
- When actual scenario (R) is realized …



Algorithm: Illustration

- Input, with $\sigma=3$
- Sample σ times from client distribution
- Build MST T_0 on S
- When actual scenario (R) is realized …
- Extend T_0 to span R



Analysis of 1st stage cost

- Let $OPT = c(T_0^*) + \sum_X p_X \sigma c(T_X^*)$

Analysis of 1st stage cost

- Let $OPT = c(T_0^*) + \sum_X p_X \sigma c(T_X^*)$
- Claim:

$$E[c(T_0)] \le 2.OPT$$

Analysis of 1st stage cost

- Let $OPT = c(T_0^*) + \sum_X p_X \sigma c(T_X^*)$
- Claim:

$$E[c(T_0)] \le 2.OPT$$

- Our σ samples: $S=\{S_1, S_2, \ldots, S_\sigma\}$

$$MST(S) \le 2\{c(T_0^*) + c(T_{S_1}^*) + \ldots + c(T_{S_\sigma}^*)\}$$

Analysis of 1st stage cost

- Let $OPT = c(T_0^*) + \sum_X p_X \sigma c(T_X^*)$
- Claim: $E[c(T_0)] \le 2.OPT$
- Our σ samples: $S=\{S_1, S_2, \ldots, S_\sigma\}$

$$MST(S) \le 2\{c(T_0^*) + c(T_{S_1}^*) + \ldots + c(T_{S_\sigma}^*)\}$$

$$E[MST(S)] \le 2\{c(T_0^*) + E[c(T_{S_1}^*)] + \ldots + E[c(T_{S_\sigma}^*)]\}$$

Analysis of 1st stage cost

- Let $OPT = c(T_0^*) + \sum_X p_X \sigma c(T_X^*)$
- Claim: $E[c(T_0)] \le 2.OPT$
- Our σ samples: $S=\{S_1, S_2, \ldots, S_\sigma\}$

$$MST(S) \le 2\{c(T_0^*) + c(T_{S_1}^*) + \ldots + c(T_{S_\sigma}^*)\}$$

$$E[MST(S)] \le 2\{c(T_0^*) + E[c(T_{S_1}^*)] + \ldots + E[c(T_{S_\sigma}^*)]\}$$

$$= 2\{c(T_0^*) + \sigma E_X[c(T_X^*)]\}$$

Analysis of 2nd stage cost

- Intuition:
  - 1st stage: σ samples at cost c_e
  - 2nd stage: *1* sample at cost $\sigma.c_e$

Analysis of 2nd stage cost

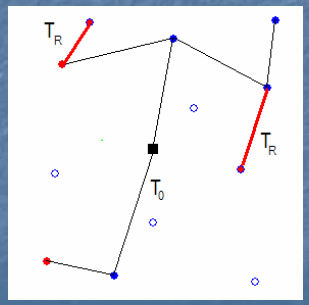
- Intuition:
  - 1st stage: σ samples at cost c_e
  - 2nd stage: *1* sample at cost $\sigma.c_e$
- In expectation,
  - 2nd stage cost ≤ 1st stage cost

Analysis of 2nd stage cost

- Intuition:
  - 1st stage: σ samples at cost c_e
  - 2nd stage: *1* sample at cost $\sigma.c_e$
- In expectation,
  - 2nd stage cost ≤ 1st stage cost
- But we've already bounded 1st stage cost!

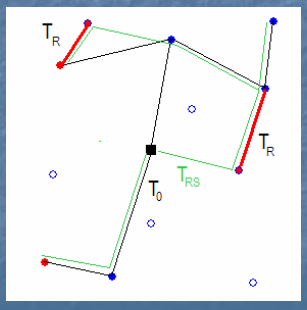
Analysis of 2nd stage cost

- Claim: $E[\sigma c(T_R)] \le E[c(T_0)]$
- Proof using an auxiliary structure



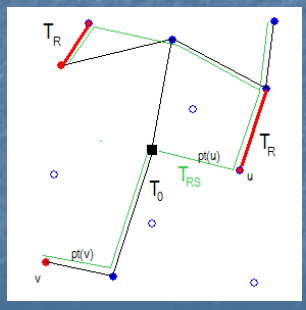
Analysis of 2nd stage cost

- Claim: $E[\sigma c(T_R)] \le E[c(T_0)]$
- Let T_{RS} be an MST on $R \cup S$



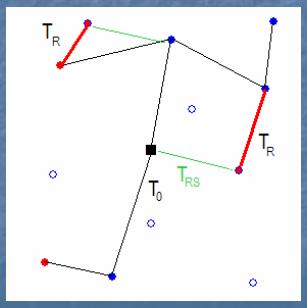
Analysis of 2nd stage cost

- Claim: $E[\sigma c(T_R)] \le E[c(T_0)]$
- Let T_{RS} be an MST on $R \cup S$
- Associate each node $v \in T_{RS}$ with its parent edge $pt(v)$; $c(T_{RS})=c(pt(R)) + c(pt(S))$



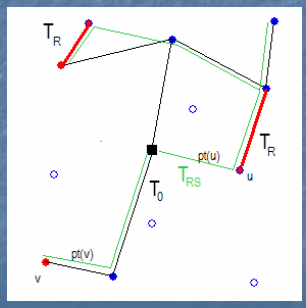
Analysis of 2nd stage cost

- Claim: $E[\sigma c(T_R)] \le E[c(T_0)]$
- Let T_{RS} be an MST on $R \cup S$
- Associate each node $v \in T_{RS}$ with its parent edge $pt(v)$; $c(T_{RS})=c(pt(R)) + c(pt(S))$
- $c(T_R) \le c(pt(R))$, since T_R was the cheapest possible way to connect R to T_0



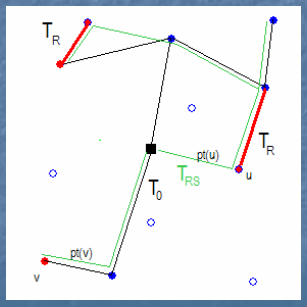
Analysis of 2nd stage cost

- Claim: $E[\sigma c(T_R)] \le E[c(T_0)]$
- Let T_{RS} be an MST on $R \cup S$
- Associate each node $v \in T_{RS}$ with its parent edge $pt(v)$; $c(T_{RS})=c(pt(R)) + c(pt(S))$
- $c(T_R) \le c(pt(R))$
- $E[c(pt(R))] \le E[c(pt(S))]/\sigma$, since R is 1 sample and S is σ samples from same process



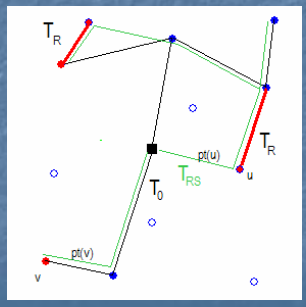
Analysis of 2nd stage cost

- Claim: $E[\sigma c(T_R)] \le E[c(T_0)]$
- Let T_{RS} be an MST on $R \cup S$
- Associate each node $v \in T_{RS}$ with its parent edge $pt(v)$; $c(T_{RS})=c(pt(R)) + c(pt(S))$
- $c(T_R) \le c(pt(R))$
- $E[c(pt(R))] \le E[c(pt(S))]/\sigma$
- $c(pt(S)) \le c(T_0)$, since $pt(S) \cup pt(R)$ is a MST while adding $pt(R)$ to T_0 spans $R \cup S$



Analysis of 2nd stage cost

- Claim: $E[\sigma c(T_R)] \le E[c(T_0)]$
- Let T_{RS} be an MST on $R \cup S$
- Associate each node $v \in T_{RS}$ with its parent edge $pt(v)$; $c(T_{RS})=c(pt(R)) + c(pt(S))$
- $c(T_R) \le c(pt(R))$
- $E[c(pt(R))] \le E[c(pt(S))]/\sigma$
- $c(pt(S)) \le c(T_0)$
- Chain inequalities and claim follows



Recap

- Algorithm for Stochastic Steiner Tree:
  - 1st stage: Sample σ times, build MST
  - 2nd stage: Extend MST to realized clients

Recap

- Algorithm for Stochastic Steiner Tree:
  - 1st stage: Sample σ times, build MST
  - 2nd stage: Extend MST to realized clients
- Theorem: Algorithm BOOST-AND-SAMPLE is a 4-approximation to Stochastic Steiner Tree

Recap

- Algorithm for Stochastic MST:
  - 1st stage: Sample σ times, build MST
  - 2nd stage: Extend MST to realized clients
- Theorem: Algorithm BOOST-AND-SAMPLE is a 4-approximation to Stochastic Steiner Tree
- Shortcomings:
  - Specific problem, in a specific model
  - Cannot adapt to scenario model with non-correlated cost changes across scenarios

Coping with shortcomings

Specific problem, in a specific model

- Boosted Sampling works for more general covering problems with subadditivity - Solves Facility location, vertex cover

Skip general model (details in STOC 04 paper)

Cannot adapt to scenario model with scenario-dependent cost inflations

- A combination of LP-rounding and primal-dual methods solves the scenario model with scenario-dependent cost inflations; Also handles risk-bounds on more general network design.

Skip scenario model (details in FOCS 04 paper)

Skip both

Outline

- Motivation: The cable company problem
- Model and literature review
- Solution to the cable company problem
- General covering problem
- Scenario dependent cost model

General Model

- U: universe of potential clients (e.g., terminals)
- X: elements which provide service, with element costs c_x (e.g., edges)
- Given $S \subseteq U$, set of feasible sol'ns is $\text{Sols}(S) \subseteq 2^X$
- Deterministic problem: Given S, find minimum cost $F \in \text{Sols}(S)$

Model: details

- Element costs are c_x in first stage and $\sigma.c_x$ in second stage
- In second stage, client set $S \subseteq U$ is realized with probability $p(S)$
- Objective: Compute F_0 and F_S to minimize
  $c(F_0) + E[\sigma\ c(F_S)]$
  where $F_0 \cup F_S \in \text{Sols}(S)$ for all S

Sampling access model

- Second stage: Client set S appears with probability $p(S)$
- We only require sampling access:
  - Oracle, when queried, gives us a sample scenario D
  - Identically distributed to actual second stage

Main result: Preview

- Given stochastic optimization problem with cost inflation factor σ :
  - Generate σ samples: $D_1, D_2, \ldots, D_\sigma$
  - Use deterministic approximation algorithm to compute $F_0 \in \text{Sols}(\cup D_i)$
  - When actual second stage S is realized, augment by selecting F_S
- Theorem: Good approximation for stochastic problem!

Requirement: Sub-additivity

- If S and S' are legal sets of clients, then:
  - $S \cup S'$ is also a legal client set
  - For any $F \in \text{Sols}(S)$ and $F' \in \text{Sols}(S')$, we also have $F \cup F' \in \text{Sols}(S \cup S')$

Requirement: Approximation

- There is an α-approximation algorithm for deterministic problem
  - Given any $S \subseteq U$, can find $F \in \text{Sols}(S)$ in polynomial time such that:
    $c(F) \leq \alpha.\min\{c(F'): F' \in \text{Sols}(S)\}$

Crucial ingredient: Cost shares

- Recall Stochastic Steiner Tree:
  - Bounding 2nd stage cost required allocating the cost of an MST to the client nodes, and summing up carefully (auxiliary structure)
- Cost sharing function: way of distributing solution cost to clients
- Originated in game theory [Young, '94], adapted to approximation algorithms [Gupta, Kumar, Pal, Roughgarden FOCS '03]

Requirement: Cost-sharing

- $\xi : 2^U \times U \rightarrow R$ is a β -strict cost sharing function for α-approximation A if:
  - $\xi(S,j) > 0$ only if $j \in S$
  - $\sum_{j \in S} \xi(S,j) \leq c(\mathrm{OPT}(S))$
  - If $S' = S \cup T$, $A(S)$ is an α-approx. for S, and $\mathrm{Aug}(S,T)$ provides a solution for augmenting $A(S)$ to also serve T, then
    $\sum_{j \in T} \xi(S',j) \geq (1/\beta)\, c(\mathrm{Aug}(S,T))$

Main theorem: Formal

- Given a sub-additive problem with α-approximation algorithm A and β-strict cost sharing function, the following is an $(\alpha+\beta)$-approximation algorithm for stochastic variant:
  - Generate σ samples: $D_1, D_2, \ldots, D_\sigma$
  - First stage: Use algorithm A to compute F_0 as an α-approximation for $\cup D_i$
  - Second stage: When actual set S is realized, use algorithm $\mathrm{Aug}(\cup D_i, S)$ to compute F_S

First-stage cost

- Samples D_i, Algo A generates $F_0 \in \mathrm{Sols}(\cup D_i)$
- Define optimum: $Z^* = c(F_0^*) + \sum_S p(S).\sigma.c(F_S^*)$
- By sub-additivity,
  $F_0^* \cup F_{D1}^* \cup \ldots \cup F_{D\sigma}^* \in \mathrm{Sols}(\cup D_i)$
- Since A is α-approximation,
  $c(F_0)/\alpha \leq c(F_0^*) + \sum_i c(F_{Di}^*)$
- $E[c(F_0)]/\alpha \leq c(F_0^*) + \sum_i E[c(F_S^*)]$
  $\leq c(F_0^*) + \sigma \sum_S p(S)\, c(F_S^*) = Z^*$
- Therefore, first-stage cost $E[c(F_0)] \leq \alpha.Z^*$

Second-stage cost

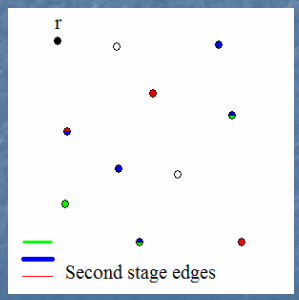
- D_i: samples, S: actual 2nd stage, define $S' = S \cup D_i$
- $c(F_S) \leq \beta.\xi(S',S)$, by cost-sharing function defn.
- $\xi(S',D_1) + \ldots + \xi(S',D_\sigma) + \xi(S',S) \leq c(\mathrm{OPT}(S'))$
- S' has $\sigma+1$ client sets, identically distributed:
  $E[\xi(S',S)] \leq E[c(\mathrm{OPT}(S'))] / (\sigma+1)$
- $c(\mathrm{OPT}(S')) \leq c(F_0^*) + c(F_{D1}^*) + \ldots + c(F_{D\sigma}^*) + c(F_S^*)$,
  by sub-additivity
- $E[c(\mathrm{OPT}(S'))] \leq c(F_0^*) + (\sigma+1)\, E[c(F_S)] \leq (\sigma+1)Z^*/\sigma$
- $E[\sigma.c(F_S)] \leq \beta.Z^*$, bounding second-stage cost

Outline

- Motivation: The cable company problem
- Model and literature review
- Solution to the cable company problem
- General covering problem
- Scenario dependent cost model

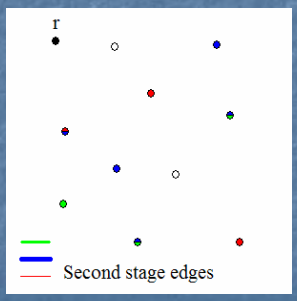
Stochastic Steiner Tree

- First stage: G, r given
- 2nd stage: one of m scenarios occurs:
  - Terminals S_k
  - Probability p_k
  - Edge cost inflation factor σ_k



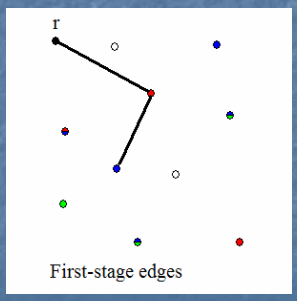
Stochastic Steiner Tree

- First stage: G, r given
- 2nd stage: one of m scenarios occurs:
  - Terminals S_k
  - Probability p_k
  - Edge cost inflation factor σ_k
- Objective: 1st stage tree T^0, 2nd stage trees T^k s.t. $T^0 \cup T^k$ span S_k



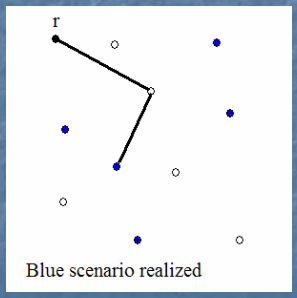
Stochastic Steiner Tree

- First stage: G, r given
- 2nd stage: one of m scenarios occurs:
  - Terminals S_k
  - Probability p_k
  - Edge cost inflation factor σ_k
- Objective: 1st stage tree T^0, 2nd stage trees T^k s.t. $T^0 \cup T^k$ span S_k



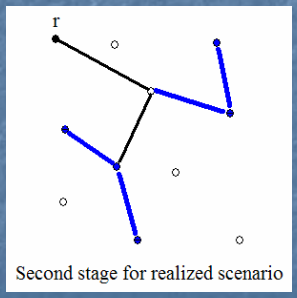
Stochastic Steiner Tree

- First stage: G, r given
- 2nd stage: one of m scenarios occurs:
  - Terminals S_k
  - Probability p_k
  - Edge cost inflation factor σ_k
- Objective: 1st stage tree T^0, 2nd stage trees T^k s.t. $T^0 \cup T^k$ span S_k



Stochastic Steiner Tree

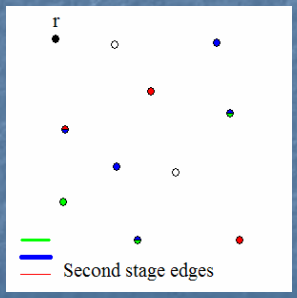
- First stage: G, r given
- 2nd stage: one of m scenarios occurs:
  - Terminals S_k
  - Probability p_k
  - Edge cost inflation factor σ_k
- Objective: 1st stage tree T^0, 2nd stage trees T^k s.t. $T^0 \cup T^k$ span S_k



Stochastic Steiner Tree

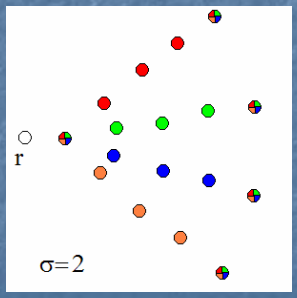
- First stage: G, r given
- 2nd stage: one of m scenarios occurs:
  - Terminals S_k
  - Probability p_k
  - Edge cost inflation factor σ_k
- Objective: 1st stage tree T^0, 2nd stage trees T^k s.t. $T^0 \cup T^k$ span S_k
- Minimize $c(T^0)+E[c(T^k)]$

Skip Algorithm



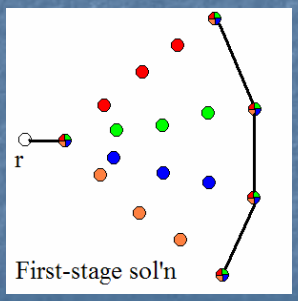
Tree solutions

- Example with 4 scenarios and $\sigma=2$



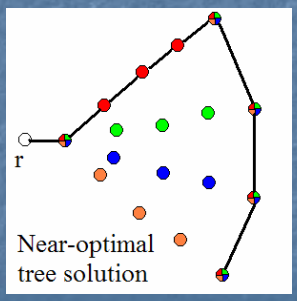
Tree solutions

- Example with 4 scenarios and $\sigma=2$
- Optimal solution may have lots of components!



Tree solutions

- Example with 4 scenarios and $\sigma=2$
- Optimal solution may have lots of components!
- Lemma: There exists a solution where 1st stage is a tree and overall cost is no more than 3 times the optimal cost
- Restrict to tree solutions



IP formulation

- Tree solution: From any (2nd-stage) terminal, path to root consists of exactly two parts: strictly 2nd-stage, followed by strictly 1st-stage
- IP: Install edges to support unit flow along such paths from each terminal to root

IP formulation

$$\min \sum_{e\in E} c(e)x_e^0 + \sum_{k=1}^{m} p_k\sigma_k \sum_{e\in E} c(e)x_e^k$$

$$\sum_{e\in\delta_+(t)} (r_e^0(t)+r_e^k(t)) \geq 1$$

$$\sum_{e\in\delta_+(v)} (r_e^0(t)+r_e^k(t)) - \sum_{e\in\delta_-(v)} (r_e^0(t)+r_e^k(t)) = 0$$

$$\sum_{e\in\delta_-(v)} r_e^0(t) - \sum_{e\in\delta_+(v)} r_e^0(t) \leq 0$$

$$r_e^k(t) - x_e^k \leq 0$$

x_e^k: edge e installed in scenario k;
$r_e^k(t)$: flow on edge e of type k from terminal t;
for $k = 0$ (1st stage) and $i=1,2,\ldots,m$ (2nd stage)

IP formulation

$$\min \sum_{e\in E} c(e)x_e^0 + \sum_{k=1}^{m} p_k\sigma_k \sum_{e\in E} c(e)x_e^k$$

$$\sum_{e\in\delta_+(t)} (r_e^0(t)+r_e^k(t)) \geq 1$$

$$\sum_{e\in\delta_+(v)} (r_e^0(t)+r_e^k(t)) - \sum_{e\in\delta_-(v)} (r_e^0(t)+r_e^k(t)) = 0$$

$$\sum_{e\in\delta_-(v)} r_e^0(t) - \sum_{e\in\delta_+(v)} r_e^0(t) \leq 0$$

$$r_e^k(t) - x_e^k \leq 0$$

Objective: minimize expected cost

IP formulation

$$\min \sum_{e\in E} c(e)x_e^0 + \sum_{k=1}^{m} p_k\sigma_k \sum_{e\in E} c(e)x_e^k$$

$$\sum_{e\in\delta_+(t)} (r_e^0(t)+r_e^k(t)) \geq 1$$

$$\sum_{e\in\delta_+(v)} (r_e^0(t)+r_e^k(t)) - \sum_{e\in\delta_-(v)} (r_e^0(t)+r_e^k(t)) = 0$$

$$\sum_{e\in\delta_-(v)} r_e^0(t) - \sum_{e\in\delta_+(v)} r_e^0(t) \leq 0$$

$$r_e^k(t) - x_e^k \leq 0$$

Unit out-flow from each terminal

IP formulation

$$\min \sum_{e \in E} c(e) x_e^0 + \sum_{k=1}^{m} p_k \sigma_k \sum_{e \in E} c(e) x_e^k$$

$$\sum_{e \in \delta_+(t)} (r_e^0(t) + r_e^k(t)) \geq 1$$

$$\sum_{e \in \delta_+(v)} (r_e^0(t) + r_e^k(t)) - \sum_{e \in \delta_-(v)} (r_e^0(t) + r_e^k(t)) = 0$$

$$\sum_{e \in \delta_-(v)} r_e^0(t) - \sum_{e \in \delta_+(v)} r_e^0(t) \leq 0$$

$$r_e^k(t) - x_e^k \leq 0$$

Flow conservation at all internal nodes ($v \neq t, r$)

IP formulation

$$\min \sum_{e \in E} c(e) x_e^0 + \sum_{k=1}^{m} p_k \sigma_k \sum_{e \in E} c(e) x_e^k$$

$$\sum_{e \in \delta_+(t)} (r_e^0(t) + r_e^k(t)) \geq 1$$

$$\sum_{e \in \delta_+(v)} (r_e^0(t) + r_e^k(t)) - \sum_{e \in \delta_-(v)} (r_e^0(t) + r_e^k(t)) = 0$$

$$\sum_{e \in \delta_-(v)} r_e^0(t) - \sum_{e \in \delta_+(v)} r_e^0(t) \leq 0$$

$$r_e^k(t) - x_e^k \leq 0$$

Flow monotonicity: enforces "First-stage must be a tree"

IP formulation

$$\min \sum_{e \in E} c(e) x_e^0 + \sum_{k=1}^{m} p_k \sigma_k \sum_{e \in E} c(e) x_e^k$$

$$\sum_{e \in \delta_+(t)} (r_e^0(t) + r_e^k(t)) \geq 1$$

$$\sum_{e \in \delta_+(v)} (r_e^0(t) + r_e^k(t)) - \sum_{e \in \delta_-(v)} (r_e^0(t) + r_e^k(t)) = 0$$

$$\sum_{e \in \delta_-(v)} r_e^0(t) - \sum_{e \in \delta_+(v)} r_e^0(t) \leq 0$$

$$r_e^k(t) - x_e^k \leq 0$$

Flow support: If an edge has flow, it must be accounted for in the objective function

IP formulation

$$\min \sum_{e \in E} c(e) x_e^0 + \sum_{k=1}^{m} p_k \sigma_k \sum_{e \in E} c(e) x_e^k$$

$$\sum_{e \in \delta_+(t)} (r_e^0(t) + r_e^k(t)) \geq 1$$

$$\sum_{e \in \delta_+(v)} (r_e^0(t) + r_e^k(t)) - \sum_{e \in \delta_-(v)} (r_e^0(t) + r_e^k(t)) = 0$$

$$\sum_{e \in \delta_-(v)} r_e^0(t) - \sum_{e \in \delta_+(v)} r_e^0(t) \leq 0$$

$$r_e^k(t) - x_e^k \leq 0$$

$$r_e^k(t), x_e^k \geq 0$$

$$r_e^k(t), x_e^k \in \{0,1\}$$

Algorithm overview

- (x,r) ← Optimal solution to LP relaxation

Algorithm overview

- (x,r) ← Optimal solution to LP relaxation
- 1st stage solution:
  - Obtain a new graph G' where $2x^0$ forms a fractional Steiner tree
  - Round using primal-dual algorithm; this is T^0

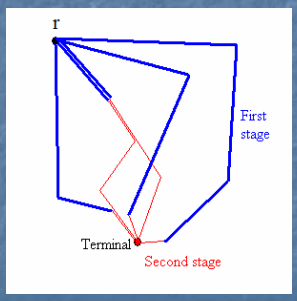
Algorithm overview

- (x,r) ← Optimal solution to LP relaxation
- 1st stage solution:
  - Obtain a new graph G' where $2x^0$ forms a fractional Steiner tree
  - Round using primal-dual algorithm; this is T^0
- 2nd stage solution:
  - Examine remaining terminals in each scenario
  - Use modified primal-dual method to obtain T^k

Skip Analysis

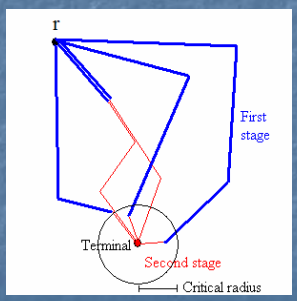
First stage

- Examine fractional paths for each terminal



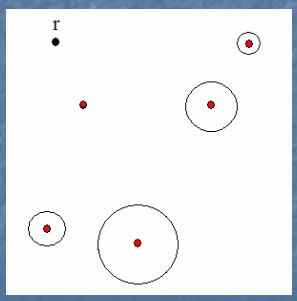
First stage

- Examine fractional paths for each terminal
- Critical radius: Flow "transitions" from 2nd-stage to 1st-stage



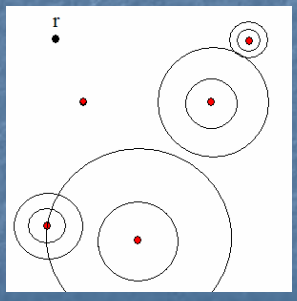
First stage

- Examine fractional paths for each terminal
- Critical radius: Flow "transitions" from 2nd-stage to 1st-stage
- Construct critical radii for all terminals



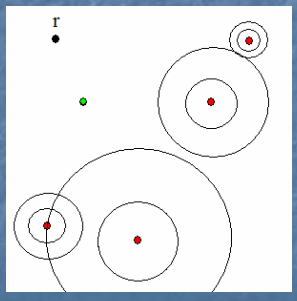
First stage

- Critical radius: Fractional flow "transitions" from 2nd-stage to 1st-stage
- Construct twice the critical radii for all terminals



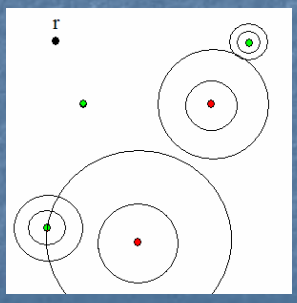
First stage

- Critical radius: Fractional flow "transitions" from 2nd-stage to 1st-stage
- Construct twice the *c.r.* for all terminals
- Examine in increasing order of *c.r.*
- R^0 ← independent set based on $2 \times$ *c.r.*



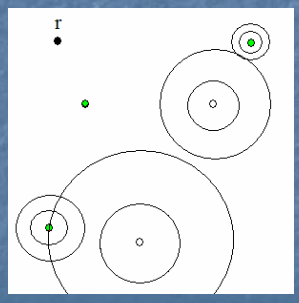
First stage

- Critical radius: Fractional flow "transitions" from 2nd-stage to 1st-stage
- Construct twice the *c.r.* for all terminals
- Examine in increasing order of *c.r.*
- $R^0 \leftarrow$ independent set based on $2 \times c.r.$



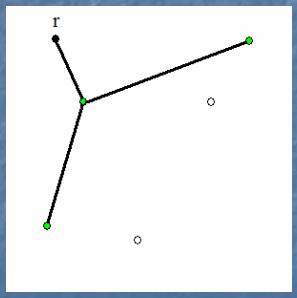
First stage

- Critical radius: Fractional flow "transitions" from 2nd-stage to 1st-stage
- Construct twice the *c.r.* for all terminals
- Examine in increasing order of *c.r.*
- $R^0 \leftarrow$ independent set based on $2 \times c.r.$



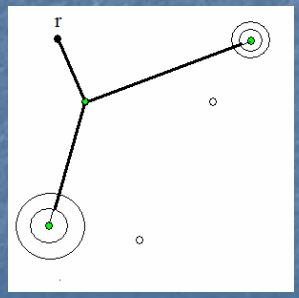
First stage

- Critical radius: Fractional flow "transitions" from 2nd-stage to 1st-stage
- Construct twice the *c.r.* for all terminals
- Examine in increasing order of *c.r.*
- $R^0 \leftarrow$ independent set based on $2 \times c.r.$
- $T^0 \leftarrow$ Steiner tree on R^0



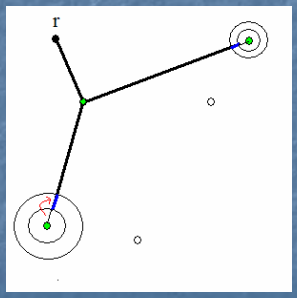
First stage analysis

- Critical radius: Fractional flow "transitions" from 2nd-stage to 1st-stage
- $R^0 \leftarrow$ independent set based on $2 \times c.r.$
- $T^0 \leftarrow$ Steiner tree on R^0
- $G' \leftarrow$ Contract *c.r.* balls around vertices in R^0
- $2x^0$ is feasible fractional Steiner tree for R^0 in G'



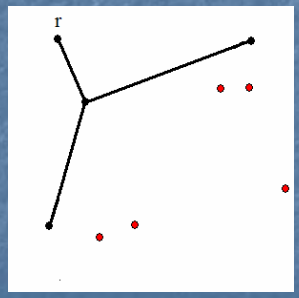
First stage analysis

- $R^0 \leftarrow$ independent set based on $2 \times c.r.$
- $T^0 \leftarrow$ Steiner tree on R^0
- $G' \leftarrow$ Contract *c.r.* balls around vertices in R^0
- $2x^0$ is feasible fractional Steiner tree for R^0 in G'
- Extension from vertex to *c.r.* charged to segment from *c.r.* to $2 \times c.r.$ (disjoint from others)



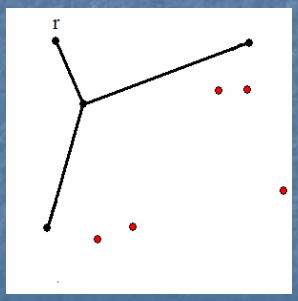
Second stage

- $T^0 \leftarrow$ 1st stage tree
- Consider scenario *k*



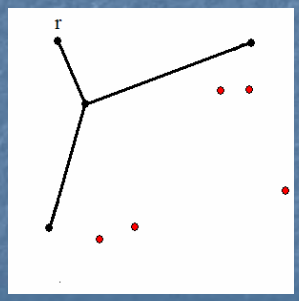
Second stage

- $T^0 \leftarrow 1^{st}$ stage tree
- Consider scenario k
- Idea: Run Steiner tree primal-dual on terminals, stopping moat M when:



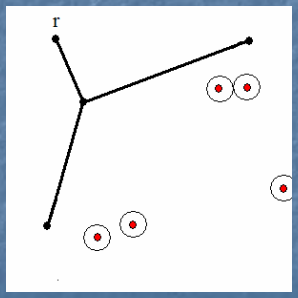
Second stage

- $T^0 \leftarrow 1^{st}$ stage tree
- Consider scenario k
- Idea: Run Steiner tree primal-dual on terminals, stopping moat M when:
  - M hits T^0
  - M hits a stopped moat
  - For every terminal in M, less than ½ flow leaving M is 2nd-stage



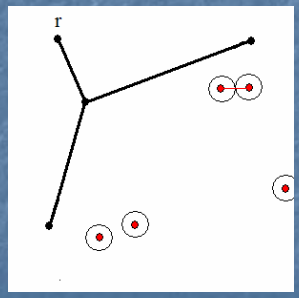
Second stage

- $T^0 \leftarrow 1^{st}$ stage tree
- Consider scenario k
- Idea: Run Steiner tree primal-dual on terminals, stopping moat M when:
  - M hits T^0
  - M hits a stopped moat
  - For every terminal in M, less than ½ flow leaving M is 2nd-stage



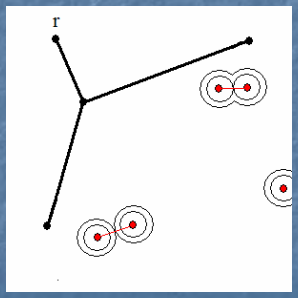
Second stage

- $T^0 \leftarrow 1^{st}$ stage tree
- Consider scenario k
- Idea: Run Steiner tree primal-dual on terminals, stopping moat M when:
  - M hits T^0
  - M hits a stopped moat
  - For every terminal in M, less than ½ flow leaving M is 2nd-stage



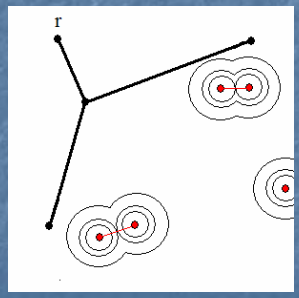
Second stage

- $T^0 \leftarrow 1^{st}$ stage tree
- Consider scenario k
- Idea: Run Steiner tree primal-dual on terminals, stopping moat M when:
  - M hits T^0
  - M hits a stopped moat
  - For every terminal in M, less than ½ flow leaving M is 2nd-stage



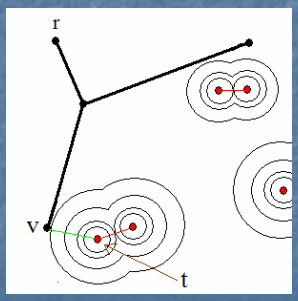
Second stage

- $T^0 \leftarrow 1^{st}$ stage tree
- Consider scenario k
- Idea: Run Steiner tree primal-dual on terminals, stopping moat M when:
  - M hits T^0
  - M hits a stopped moat
  - For every terminal in M, less than ½ flow leaving M is 2nd-stage



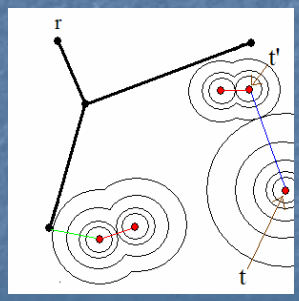
Second stage

- Idea: Run Steiner tree primal-dual on terminals, stopping moat M when:
  - M hits T^0
  - M hits a stopped moat
  - For every terminal in M, less than ½ flow leaving M is 2nd-stage
- If M hits T^0, add edge from $t \in M$ to $v \in R^0$



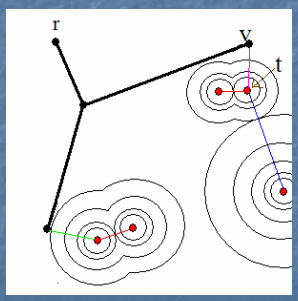
Second stage

- Idea: Run Steiner tree primal-dual on terminals, stopping moat M when:
  - M hits T^0
  - M hits a stopped moat
  - For every terminal in M, less than ½ flow leaving M is 2nd-stage
- If M hits M', connect $t \in M$ with $t' \in M'$ as in Steiner tree primal-dual



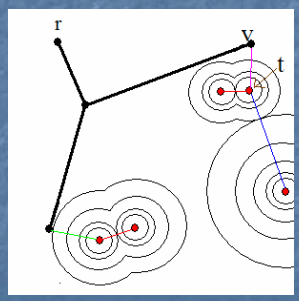
Second stage

- Idea: Run Steiner tree primal-dual on terminals, stopping moat M when:
  - M hits T^0
  - M hits a stopped moat
  - For every terminal in M, less than ½ flow leaving M is 2nd-stage
- There exists $t \in M$ and $v \in R^0$ s.t. v within $4 \times$ c.r. of t; connect t to v



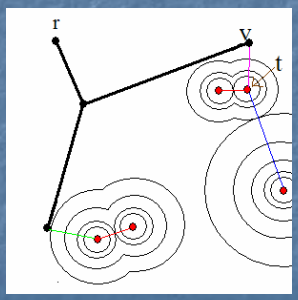
Second stage analysis

- Primal-dual accounts for edges inside moats



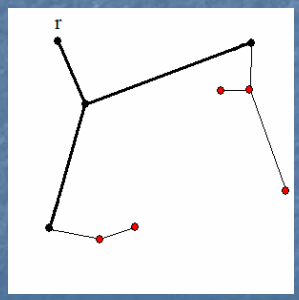
Second stage analysis

- Primal-dual accounts for edges inside moats
- Connector edges paid by carefully accounting:
  - Primal-dual bound
  - For every terminal t, there is $v \in R^0$ within $4 \times$ c.r. of t



SST: main result

- 24-approximation for Stochastic Steiner Tree (Improvement to 16-approx possible)
- Method: Primal-dual overlaid on LP solution
- Extensions to more general network design with routing costs
- Per-scenario risk-bounds incorporated and rounded



Main Techniques in other results

- Stochastic Facility Location – Rounding natural LP formulation using filter-and-round (Lin-Vitter, Shmoys-Tardos-Aardal) carefully [Details in IPCO '04]
- Stochastic Minimum Spanning Tree – Both scenario and black-box models - Randomized rounding of natural LP formulation gives nearly best possible O(log [No. of vertices] + log [max cost/min cost of an edge across scenarios]) approximation result [Details in IPCO '05]
- Multi-stage general covering problems – Boosted sampling with rejection based on ratio of scenario's inflation to maximum possible works [manuscript]

Summary

- Natural boosted sampling algorithm works for a broad class of stochastic problems in black-box model
- Boosted sampling with rejection extends to multi-stage covering problems in the black-box model
- Existing techniques can be cleverly adapted for the scenario model (E.g., LP-rounding for Facility location, primal-dual for Vertex Covers, combination of both for Steiner trees)
- Randomized rounding of LP formulations works for black-box formulation of spanning trees

More approximation algorithms for stochastic programming programs

David B. Shmoys

Joint work with Chaitanya Swamy
Cal Tech

Stochastic Optimization

- Way of modeling uncertainty.
- Exact data is unavailable or expensive – data is uncertain, specified by a probability distribution.

  Want to make the best decisions given this uncertainty in the data.
- Dates back to 1950's and the work of Dantzig.
- Applications in logistics, transportation models, financial instruments, network design, production planning, …

Two-Stage Recourse Model

Given : Probability distribution over inputs.

Stage I : Make some advance decisions – plan ahead or hedge against uncertainty.

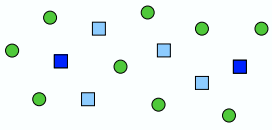
Observe the actual input scenario.

Stage II : Take recourse. Can augment earlier solution paying a recourse cost.

Choose stage I decisions to minimize

(stage I cost) + (expected stage II recourse cost).

2-Stage Stochastic Facility Location



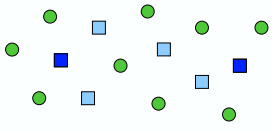
facility stage I facility
client set D

Distribution over clients gives the set of clients to serve.

Stage I: Open some facilities in advance; pay cost f_i for facility i.

Stage I cost = $\sum_{(i \text{ opened})} f_i$.

2-Stage Stochastic Facility Location



facility stage I facility
client set D

Distribution over clients gives the set of clients to serve.

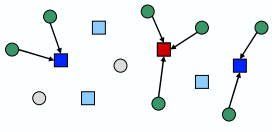
Stage I: Open some facilities in advance; pay cost f_i for facility i.

Stage I cost = $\sum_{(i \text{ opened})} f_i$.

How is the probability distribution on clients specified?

- A short (polynomial) list of possibile scenarios;
- Independent probabilities that each client exists;
- A black box that can be sampled.

2-Stage Stochastic Facility Location



facility stage I facility

Distribution over clients gives the set of clients to serve.

Stage I: Open some facilities in advance; pay cost f_i for facility i.

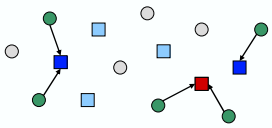
Stage I cost = $\sum_{(i \text{ opened})} f_i$.

Actual scenario A = { clients to serve}, materializes.

Stage II: Can open more facilities to serve clients in A; pay cost f_i^A to open facility i. Assign clients in A to facilities.

Stage II cost = $\sum_{\substack{i \text{ opened in} \\ \text{scenario } A}} f_i^A$ + (cost of serving clients in A).

2-Stage Stochastic Facility Location



facility stage I facility

Distribution over clients gives the set of clients to serve.

Stage I: Open some facilities in advance; pay cost f_i for facility i.

Stage I cost = $\Sigma_{(i \text{ opened})} f_i$.

Actual scenario A = {clients to serve}, materializes.

Stage II: Can open more facilities to serve clients in A; pay cost f_i^A to open facility i. Assign clients in A to facilities.

Stage II cost = $\Sigma_{i \text{ opened in scenario } A} f_i^A$ + (cost of serving clients in A).

Want to decide which facilities to open in stage I.

Goal: Minimize Total Cost =

(stage I cost) + $E_{A \subseteq D}$ [stage II cost for A].

We want to prove a worst-case guarantee.

Give an algorithm that "works well" on any instance, and for any probability distribution.

A is an α-approximation algorithm if -

- A runs in polynomial time;
- $A(I) \leq \alpha . OPT(I)$ on all instances I.

α is called the approximation ratio of A.

What is new here?

- Previous "black box" results all assumed that, for each element of the solution (facility opened, edge in Steiner tree) the costs in the two stages are proportional: (stage II cost) = λ(stage I cost).
- Note: λ in this talk is the same as σ in previous one
- We allow independent stage I and stage II costs
- Previous results rely on structure of underlying stochastic LPs; we will provide algorithms to (approximately) solve those LPs

Our Results

- Give the first approximation algorithms for 2-stage discrete stochastic problems
  - black-box model
  - no assumptions on costs.
- Give a fully polynomial randomized approximation scheme for a large class of 2-stage stochastic linear programs (contrast to Kleywegt, Shapiro, & Homem-DeMillo 01, Dyer, Kannan & Stougie 02, Nesterov & Vial 00)
- Give another way to "reduce" stochastic optimization problems to their deterministic versions.

Stochastic Set Cover (SSC)

Universe $U = \{e_1, \ldots, e_n\}$, subsets $S_1, S_2, \ldots, S_m \subseteq U$, set S has weight w_S.

Deterministic problem: Pick a minimum weight collection of sets that covers each element.

Stochastic version: Set of elements to be covered is given by a probability distribution.

- choose some sets initially paying w_S for set S
- subset $A \subseteq U$ to be covered is revealed
- can pick additional sets paying w_S^A for set S.

Minimize (w-cost of sets picked in stage I) +

$E_{A \subseteq U}$ [w^A-cost of new sets picked for scenario A].

An LP formulation

For simplicity, consider $w_S^A = w_S$ for every scenario A.

p_A : probability of scenario $A \subseteq U$.

x_S : indicates if set S is picked in stage I.

$y_{A,S}$: indicates if set S is picked in scenario A.

Minimize $\Sigma_S w_S x_S + \Sigma_{A \subseteq U} p_A \Sigma_S w_S y_{A,S}$

subject to,

$\Sigma_{S: e \in S} x_S + \Sigma_{S: e \in S} y_{A,S} \geq 1$ for each $A \subseteq U$, $e \in A$

$x_S, y_{A,S} \geq 0$ for each S, A.

Exponential number of variables and exponential number of constraints.

A Rounding Theorem

Stochastic Problem: LP can be solved in polynomial time.

Example: polynomial scenario setting

Deterministic problem: α-approximation algorithm A with respect to the LP relaxation, $A(I) \le \alpha \cdot \text{LP-OPT}(I)$ for each I.

Example: "the greedy algorithm" for set cover is a $\log n$-approximation algorithm w.r.t. LP relaxation.

Theorem: Can use such an α-approx. algorithm to get a 2α-approximation algorithm for stochastic set cover.

Rounding the LP

Assume LP can be solved in polynomial time.
Suppose we have an α-approximation algorithm wrt. the LP relaxation for the deterministic problem.

Let (x,y) : optimal solution with cost LP-OPT.

$\sum_{S: e \in S} x_S + \sum_{S: e \in S} y_{A,S} \ge 1$ for each $A \subseteq U$, $e \in A$

$\Rightarrow$ for every element e, either

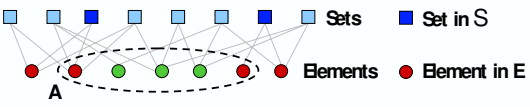
$\sum_{S: e \in S} x_S \ge \frac{1}{2}$ OR in each scenario $A : e \in A$, $\sum_{S: e \in S} y_{A,S} \ge \frac{1}{2}$.

Let $E = \{e : \sum_{S: e \in S} x_S \ge \frac{1}{2}\}$.

So (2x) is a fractional set cover for the set E $\Rightarrow$ can "round" to get an integer set cover S for E of cost $\sum_{S \in S} \omega_S \le \alpha(\sum_S 2\omega_S x_S)$.

S is the first stage decision.

Rounding (contd.)



Consider any scenario A. Elements in $A \cap E$ are covered.

For every $e \in A \setminus E$, it must be that $\sum_{S: e \in S} y_{A,S} \ge \frac{1}{2}$.
So $(2y^A)$ is a fractional set cover for $A \setminus E \Rightarrow$ can round to get a set cover of W-cost $\le \alpha(\sum_S 2W_S y_{A,S})$.

Using this to augment S in scenario A, expected cost

$\le \sum_{S \in S} \omega_S + 2\alpha \cdot \sum_{A \subseteq U} p_A (\sum_S W_S y_{A,S}) \le 2\alpha \cdot$ LP-OPT.

A Rounding Theorem

Stochastic Problem: LP can be solved in polynomial time.

Example: polynomial scenario setting

Deterministic problem: α-approximation algorithm A with respect to the LP relaxation, $A(I) \le \alpha \cdot \text{LP-OPT}(I)$ for each I.

Example: "the greedy algorithm" for set cover is a $\log n$-approximation algorithm w.r.t. LP relaxation.

Theorem: Can use such an α-approx. algorithm to get a 2α-approximation algorithm for stochastic set cover.

A Rounding Technique

Assume LP can be solved in polynomial time.
Suppose we have an α-approximation algorithm w.r.t. the LP relaxation for the deterministic problem.

Let (x,y) : optimal solution with cost OPT.

$\sum_{S: e \in S} x_S + \sum_{S: e \in S} y_{A,S} \ge 1$ for each $A \subseteq U$, $e \in A$

$\Rightarrow$ for every element e, either

$\sum_{S: e \in S} x_S \ge \frac{1}{2}$ OR in each scenario $A : e \in A$, $\sum_{S: e \in S} y_{A,S} \ge \frac{1}{2}$.

Let $E = \{e : \sum_{S: e \in S} x_S \ge \frac{1}{2}\}$.

So (2x) is a fractional set cover for the set E $\Rightarrow$ can "round" to get an integer set cover S of cost $\sum_{S \in S} \omega_S \le \alpha(\sum_S 2\omega_S x_S)$.

S is the first stage decision.

A Compact Formulation

p_A : probability of scenario $A \subseteq U$.
x_S : indicates if set S is picked in stage I.

Minimize $h(x) = \sum_S \omega_S x_S + f(x)$ s.t. $x_S \ge 0$ for each S

where, $f(x) = \sum_{A \subseteq U} p_A f_A(x)$

and $f_A(x) = \min. \sum_S W_S y_{A,S}$

s.t. $\sum_{S: e \in S} y_{A,S} \ge 1 - \sum_{S: e \in S} x_S$ for each $e \in A$

Equivalent to earlier LP! $y_{A,S} \ge 0$ for each S.

Each $f_A(x)$ is convex, so f(x) and h(x) are convex functions.

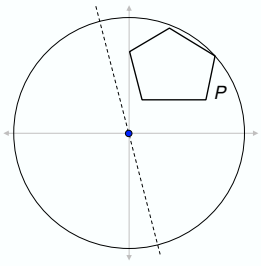
The Algorithm

1. Get a $(1+\varepsilon)$-optimal solution $(\mathbf{x})$ to compact convex program using the ellipsoid method.
2. Round $(\mathbf{x})$ using a $\log n$-approx. algorithm for the deterministic problem to decide which sets to pick in stage I.

Obtain a $(2\log n+\varepsilon)$-approximation algorithm for the stochastic set cover problem.

The Ellipsoid Method

Min $\mathbf{c}\cdot\mathbf{x}$ subject to $\mathbf{x}\in P$.



Ellipsoid ≡ squashed sphere

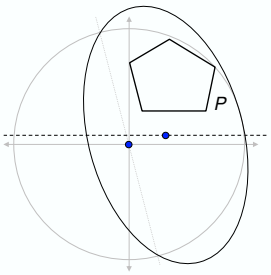
Start with ball containing polytope P.

$\mathbf{y}_i$ = center of current ellipsoid.

If $\mathbf{y}_i$ is infeasible, use violated inequality to chop off infeasible half-ellipsoid.

The Ellipsoid Method

Min $\mathbf{c}\cdot\mathbf{x}$ subject to $\mathbf{x}\in P$.



Ellipsoid ≡ squashed sphere

Start with ball containing polytope P.

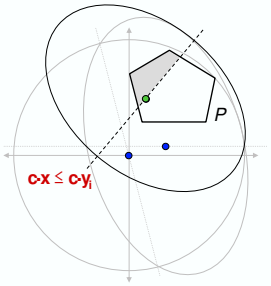
$\mathbf{y}_i$ = center of current ellipsoid.

If $\mathbf{y}_i$ is infeasible, use violated inequality to chop off infeasible half-ellipsoid.

New ellipsoid = min. volume ellipsoid containing "unchopped" half-ellipsoid.

The Ellipsoid Method

Min $\mathbf{c}\cdot\mathbf{x}$ subject to $\mathbf{x}\in P$.



Ellipsoid ≡ squashed sphere

Start with ball containing polytope P.

$\mathbf{y}_i$ = center of current ellipsoid.

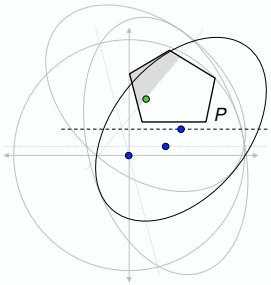
If $\mathbf{y}_i$ is infeasible, use violated inequality to chop off infeasible half-ellipsoid.

If $\mathbf{y}_i \in P$, use objective function cut $\mathbf{c}\cdot\mathbf{x} \le \mathbf{c}\cdot\mathbf{y}_i$ to chop off polytope, half-ellipsoid.

New ellipsoid = min. volume ellipsoid containing "unchopped" half-ellipsoid.

The Ellipsoid Method

Min $\mathbf{c}\cdot\mathbf{x}$ subject to $\mathbf{x}\in P$.



Ellipsoid ≡ squashed sphere

Start with ball containing polytope P.

$\mathbf{y}_i$ = center of current ellipsoid.

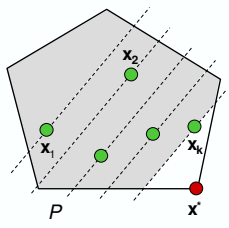
If $\mathbf{y}_i$ is infeasible, use violated inequality to chop off infeasible half-ellipsoid.

If $\mathbf{y}_i \in P$, use objective function cut $\mathbf{c}\cdot\mathbf{x} \le \mathbf{c}\cdot\mathbf{y}_i$ to chop off polytope, half-ellipsoid.

New ellipsoid = min. volume ellipsoid containing "unchopped" half-ellipsoid.

The Ellipsoid Method

Min $\mathbf{c}\cdot\mathbf{x}$ subject to $\mathbf{x}\in P$.



Ellipsoid ≡ squashed sphere

Start with ball containing polytope P.

$\mathbf{y}_i$ = center of current ellipsoid.

If $\mathbf{y}_i$ is infeasible, use violated inequality to chop off infeasible half-ellipsoid.

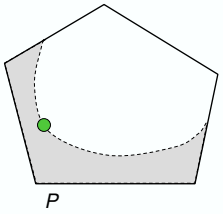
If $\mathbf{y}_i \in P$, use objective function cut $\mathbf{c}\cdot\mathbf{x} \le \mathbf{c}\cdot\mathbf{y}_i$ to chop off polytope, half-ellipsoid.

New ellipsoid = min. volume ellipsoid containing "unchopped" half-ellipsoid.

$\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k$: points lying in P. $\mathbf{c}\cdot\mathbf{x}_k$ is a close to optimal value.

Ellipsoid for Convex Optimization

Min $h(x)$ subject to $x \in P$.



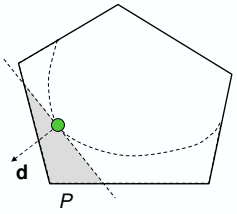
Start with ball containing polytope P.
y_i = center of current ellipsoid.

If y_i is infeasible, use violated inequality.

If $y_i \in P$ – how to make progress?
add inequality $h(x) \le h(y_i)$? Separation becomes difficult.

Ellipsoid for Convex Optimization

Min $h(x)$ subject to $x \in P$.



Start with ball containing polytope P.
y_i = center of current ellipsoid.

If y_i is infeasible, use violated inequality.

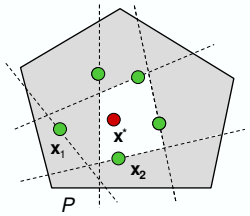
If $y_i \in P$ – how to make progress?
add inequality $h(x) \le h(y_i)$? Separation becomes difficult.
Let d = subgradient at y_i.
use subgradient cut $d \cdot (x - y_i) \le 0$.

Generate new min. volume ellipsoid.

$d \in \Re^n$ is a subgradient of $h(.)$ at u, if for every v, $h(v) - h(u) \ge d \cdot (v - u)$.

Ellipsoid for Convex Optimization

Min $h(x)$ subject to $x \in P$.



Start with ball containing polytope P.
y_i = center of current ellipsoid.

If y_i is infeasible, use violated inequality.

If $y_i \in P$ – how to make progress?
add inequality $h(x) \le h(y_i)$? Separation becomes difficult.
Let d = subgradient at y_i.
use subgradient cut $d \cdot (x - y_i) \le 0$.

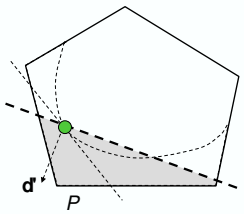
Generate new min. volume ellipsoid.

$d \in \Re^n$ is a subgradient of $h(.)$ at u, if for every v, $h(v) - h(u) \ge d \cdot (v - u)$.

$x_1, x_2, \ldots, x_k$: points in P. Can show, $\min_{i=1\ldots k} h(x_i) \le OPT + \rho$.

Ellipsoid for Convex Optimization

Min $h(x)$ subject to $x \in P$.



Start with ball containing polytope P.
y_i = center of current ellipsoid.

If y_i is infeasible, use violated inequality.

If $y_i \in P$ – how to make progress?
add inequality $h(x) \le h(y_i)$? Separation becomes difficult.
subgradient is difficult to compute.
Let d' = ε-subgradient at y_i.
use ε-subgradient cut $d' \cdot (x - y_i) \le 0$.

$d' \in \Re^n$ is a ε-subgradient of $h(.)$ at u, if $\forall v \in P$, $h(v) - h(u) \ge d' \cdot (v - u) - \varepsilon \cdot h(u)$.

$x_1, x_2, \ldots, x_k$: points in P. Can show, $\min_{i=1\ldots k} h(x_i) \le OPT/(1-\varepsilon) + \rho$.

Subgradients and ε-subgradients

Vector d is a subgradient of $h(.)$ at u,
if for every v, $h(v) - h(u) \ge d \cdot (v - u)$.

Vector d' is an ε-subgradient of $h(.)$ at u,
if for every $v \in P$, $h(v) - h(u) \ge d' \cdot (v - u) - \varepsilon \cdot h(u)$.

$P = \{ x : 0 \le x_S \le 1$ for each set $S \}$.

$h(x) = \sum_S \omega_S x_S + \sum_{A \subseteq U} p_A f_A(x) = \omega \cdot x + \sum_{A \subseteq U} p_A f_A(x)$

Lemma: Let d be a subgradient at u, and d' be a vector such that $d_S - \varepsilon \omega_S \le d'_S \le d_S$ for each set S. Then, d' is an ε-subgradient at point u.

Getting a "nice" subgradient

$h(x) = \omega \cdot x + \sum_{A \subseteq U} p_A f_A(x)$

$f_A(x) =$ min. $\sum_S W_S y_{A,S}$

s.t. $\sum_{S e \in S} y_{A,S} \ge 1 - \sum_{S e \in S} x_S$
$\forall e \in A$

$y_{A,S} \ge 0 \quad \forall S$

Getting a "nice" subgradient

$h(x) = \omega \cdot x + \sum_{A \subseteq U} p_A f_A(x)$

$f_A(x) =$ min. $\sum_S w_S y_{A,S}$ = max. $\sum_{e \in A} (1 - \sum_{S \ni e} x_S) z_{A,e}$

st. $\sum_{S \ni e} y_{A,S} \geq 1 - \sum_{S \ni e} x_S$ st. $\sum_{e \in A \cap S} z_{A,e} \leq w_S$

$\forall e \in A$ $\forall S$

$y_{A,S} \geq 0$ $\forall S$ $z_{A,e} \geq 0$ $\forall e \in A$

Getting a "nice" subgradient

$h(x) = \omega \cdot x + \sum_{A \subseteq U} p_A f_A(x)$

$f_A(x) =$ min. $\sum_S w_S y_{A,S}$ = max. $\sum_e (1 - \sum_{S \ni e} x_S) z_{A,e}$

st. $\sum_{S \ni e} y_{A,S} \geq 1 - \sum_{S \ni e} x_S$ st. $\sum_{e \in S} z_{A,e} \leq w_S$

$\forall e \in A$ $\forall S$

$y_{A,S} \geq 0$ $\forall S$ $z_{A,e} = 0$ $\forall e \notin A$, $z_{A,e} \geq 0$ $\forall e$

Consider point $u \in \Re^n$. Let $z_A \equiv$ optimal dual solution for A at u.

Lemma: For any point $v \in \Re^n$, we have $h(v) - h(u) \geq d \cdot (v-u)$ where $d_S = \omega_S - \sum_{A \subseteq U} p_A \sum_{e \in S} z_{A,e}$.

$\Rightarrow$ d is a subgradient of $h(.)$ at point u.

Computing an ε-Subgradient

Given point $u \in \Re^n$. $z_A \equiv$ optimal dual solution for A at u.

Subgradient at u: $d_S = \omega_S - \sum_{A \subseteq U} p_A \sum_{e \in S} z_{A,e}$.

Want: d' such that $d_S - \varepsilon\omega_S \leq d'_S \leq d_S$ for each S.

For each S, $-W_S \leq d_S \leq \omega_S$. Let $\lambda = \max_S W_S/\omega_S$.

Sample once from black box to get random scenario A.

Compute X with $X_S = \omega_S - \sum_{e \in S} z_{A,e}$.

$E[X_S] = d_S$ and $Var[X_S] \leq W_S^2$.

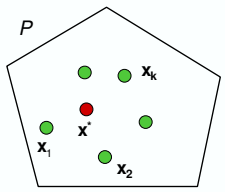
Sample $O(\lambda^2/\varepsilon^2 \cdot \log(n/\delta))$ times to compute d' such that

$Pr[\forall S, d_S - \varepsilon\omega_S \leq d'_S \leq d_S] \geq 1-\delta$.

$\Rightarrow$ d' is an ε-subgradient at u with probability $\geq 1-\delta$.

Putting it all together

Min $h(x)$ subject to $x \in P$.



✓ Can compute ε-subgradients.

Run ellipsoid algorithm.

Given y_i = center of current ellipsoid.

If y_i is infeasible, use violated inequality as a cut.

If $y_i \in P$ use ε-subgradient cut.

Continue with smaller ellipsoid.

Generate points $x_1, x_2, \ldots, x_k$ in P. Return $\bar{x} = \text{argmin}_{i=1\ldots k} h(x_i)$.

Get that $h(\bar{x}) \leq OPT/(1-\varepsilon) + \rho$.

Finally,

Get solution x with $h(x)$ close to OPT.

Sample initially to detect if $OPT = \Omega(1/\lambda)$ – this allows one to get a $(1+\varepsilon)$-OPT guarantee.

Theorem: Compact convex program can be solved to within a factor of $(1+\varepsilon)$ in polynomial time, with high probability.

Gives a $(2\log n+\varepsilon)$-approximation algorithm for the stochastic set cover problem.

A Solvable Class of Stochastic LPs

Minimize $h(x) = w.x + \sum_{A \subseteq U} p_A f_A(x)$

st. $x \in \Re^n$, $x \geq 0$, $x \in P$

where $f_A(x) =$ min. $w^A.y_A + c^A.r_A$

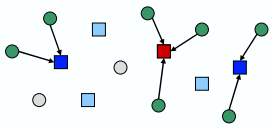
st. $B r_A \geq j^A$

$D r_A + T y_A \geq /^A - Tx$

$y_A \in \Re^n$, $r_A \in \Re^m$, $y_A \geq 0$, $r_A \geq 0$.

Theorem: Can get a $(1+\varepsilon)$-optimal solution for this class of stochastic programs in polynomial time.

2-Stage Stochastic Facility Location



□ facility ■ stage I facility

Distribution over clients gives the set of clients to serve.

Stage I: Open some facilities in advance; pay cost f_i for facility i.

Stage I cost = $\sum_{(i \text{ opened})} f_i$.

Actual scenario A = { ● clients to serve}, materializes.

Stage II: Can open more facilities to serve clients in A; pay cost f_i^A to open facility i. Assign clients in A to facilities.

Stage II cost = $\sum_{\substack{i \text{ opened in} \\ \text{scenario A}}} f_i^A$ + (cost of serving clients in A).

A Convex Program

p_A : probability of scenario $A \subseteq D$.
y_i : indicates if facility i is opened in stage I.
$y_{A,i}$: indicates if facility i is opened in scenario A.
$x_{A,ij}$: whether client j is assigned to facility i in scenario A.

Minimize $h(y) = \sum_i f_i y_i + g(y)$ s.t. $y_i \geq 0$ for each i

(SUFL-P)

where, $g(y) = \sum_{A \subseteq D} p_A g_A(y)$

and $g_A(y) = \min. \sum_i F_i y_{A,i} + \sum_{j,i} c_{ij} x_{A,ij}$

s.t. $\sum_i x_{A,ij} \geq 1$ for each $j \in A$

$x_{A,ij} \leq y_i + y_{A,i}$ for each i,j

$x_{\cdot\cdot}, y_{\cdot\cdot} \geq 0$ for each i,j.

Moral of the Story

- Even though the Stochastic LP relaxation has an exponential number of variables and constraints, we can still obtain near-optimal solutions to fractional first-stage decisions
- Fractional first-stage decisions are sufficient to decouple the two stages near-optimally
- Many applications: multicommodity flows, vertex cover, facility location, …
- But we still have to solve convex program with many, many samples (not just λ)!

Sample Average Approximation

Sample Average Approximation (SAA) method:
- Sample initially N times from scenario distribution
- Solve 2-stage problem estimating p_A with frequency of occurrence of scenario A

How large should N be?

Kleywegt, Shapiro & Homem De-Mello (KSH01):
- bound N by variance of a certain quantity – need not be polynomially bounded even for our class of programs.

SwamyS:
- show using ε-subgradients that for our class, N can be poly-bounded.

Nemirovskii & Shapiro:
- show that for SSC with non-scenario dependent costs, KSH01 gives polynomial bound on N for (preprocessing + SAA) algorithm.

Sample Average Approximation

Sample Average Approximation (SAA) method:
- Sample N times from distribution
- Estimate p_A by q_A = frequency of occurrence of scenario A

(P) $\min_{x \in P} (h(x) = \omega \cdot x + \sum_{A \subseteq U} p_A f_A(x))$

(SAA-P) $\min_{x \in P} (h'(x) = \omega \cdot x + \sum_{A \subseteq U} q_A f_A(x))$

To show: With poly-bounded N, if $\bar{x}$ solves (SAA-P) then $h(\bar{x}) \approx OPT$.

Let $z_A \equiv$ optimal dual solution for scenario A at point $u \in \Re^m$.
$\Rightarrow d_u$ with $d_{uS} = \omega_S - \sum_{A \subseteq U} q_A \sum_{e \in S} z_{A,e}$ is a subgradient of $h'(.)$ at u.

Lemma: With high probability, for "many" points u in P,
d_u is a subgradient of $h'(.)$ at u,
d_u is an approximate subgradient of $h(.)$ at u.

Establishes "closeness" of $h(.)$ and $h'(.)$ and suffices to prove result.

Intuition: Can run ellipsoid on both (P) and (SAA-P) using the same vector d_u at feasible point u.

Multi-stage Problems

Given : Distribution over inputs.

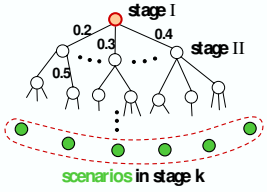
Stage I : Make some advance decisions – hedge against uncertainty.

Uncertainty evolves in various stages.

Learn new information in each stage.

Can take recourse actions in each stage – can augment earlier solution paying a recourse cost.

k-stage problem ≡ k decision points



Multi-stage Problems

Given : Distribution over inputs.

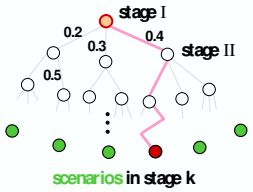
Stage I : Make some advance decisions – hedge against uncertainty.

Uncertainty evolves in various stages.

Learn new information in each stage.

Can take recourse actions in each stage – can augment earlier solution paying a recourse cost.

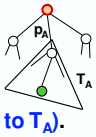
k-stage problem
≡ k decision points



Choose stage I decisions to minimize expected total cost =

(stage I cost) + $E_{\text{all scenarios}}$ [cost of stages 2 … k].

Solving k-stage LPs



Consider 3-stage SSC.

How to compute an ε-subgradient?

Want to get d' that is component-wise close to subgradient d where $d_S = \omega_S - \sum_A p_A$(dual solution to T_A).

Problem: To compute d (even in expectation) need to solve the dual of a 2-stage LP – dual has exponential size!

Fix:

- Formulate a new compact non-linear dual of polynomial size.
- Dual has a 2-stage primal LP embedded inside – solve this using earlier algorithm.

Recursively apply this idea to solve k-stage stochastic LPs.

This is just the beginning!

- Multi-stage problems with a variable number of stages
- [Dean, Goemans, Vondrak 04] Stochastic knapsack problem – in each stage decide whether to pack next item
- [Levi, Pal, Roundy, Shmoys 05] Stochastic inventory control problems – in each stage react to updated forecast of future demand
- Stochastic Dynamic Programming ???

Thank You.

Efficient Haplotype Inference on Pedigrees and Applications

Tao Jiang
Dept of Computer Science
University of California – Riverside
(joint work with Jing Li, CWRU)

1

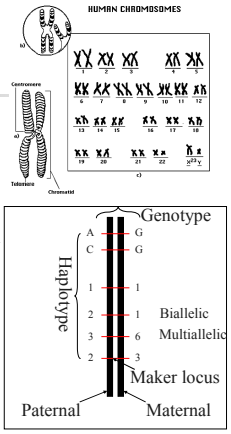
Outline

- Background
- The MRHC problem and complexity
- An exact algorithm for 0-recombinant data
- A heuristic algorithm (block-extension)
- Integer linear programming formulation and solution for MRHC with missing alleles
- Experimental results and application in disease gene association mapping
- Inference of haplotypes on population data

2

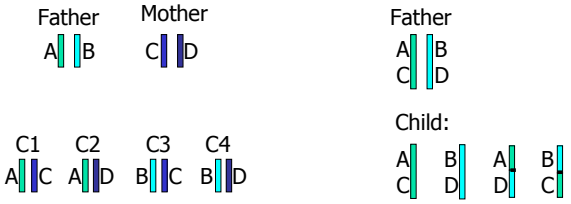
Terms

- Diploid
- Polymorphisms, marker, allele, and SNP
- Genotype, homozygous & heterozygous
- Haplotype, paternal & maternal haplotypes



3

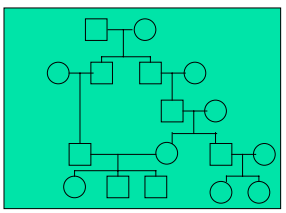
Mendelian Law of Inheritance and Recombination

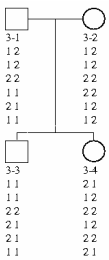


4

Pedigree

- **Pedigree, nuclear family, founder**

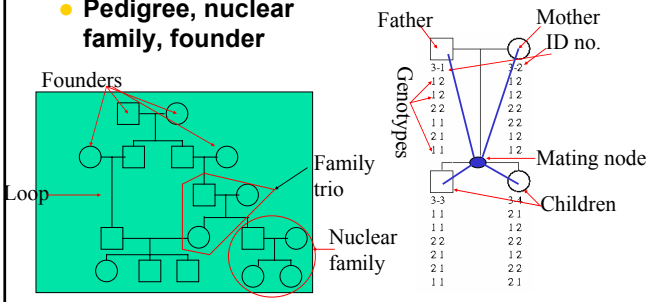




5

Pedigree

- **Pedigree, nuclear family, founder**



6

Haplotyping from Genotypes: The Problem & Methods

- **Problem:**
  - **Input: genotype data (possibly with missing alleles).**
  - **Output: haplotypes.**
- **Input data:**
  - **Data with pedigree (dependent individuals).**
  - **Data without pedigree info (independent individuals).**
- **Statistical methods**
  - **Find the most likely haplotypes based on genotype data.**
  - **Adv: solid theoretical bases**
  - **Disadv: computation intensive**
- **Rule-based (*i.e.* combinatorial) methods**
  - **Define rules/objective functions based on some plausible assumptions and find haplotypes consistent with the rules or optimizing the obj. fun.**
  - **Adv: usually simple thus very fast**
  - **Disadv: no numerical assessment of the reliability of the results**

7

Motivations

- Haplotype is more biologically meaningful than genotype since haplotypes are directly inherited from parents. Haplotype data is more informative in the studies of association between diseases and genes, and human history.
- The human genome project gives us the consensus genotype sequence of humans, but in order to understand the genetic effects on many complex diseases such as cancers, diabetes, osteoporoses, genetic variations are more important, which is best refecledt in haplotypes.
- Current experimental techniques collect genotype data. Computational methods deriving haplotypes from genotypes are highly demanded.
- The ongoing international HapMap project.

8

Motivations (cont'd)

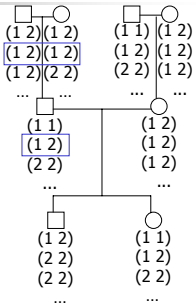
- It is generally believed that with parents/pedigree information, we could get more accurate haplotype and frequency estimations than from data without such information (*i.e.* population data).
- Family-based association studies have been widely used. We would expect more family-based gene mapping methods that assume accurate haplotype information.
- Not only computation intensive, model-based statistical methods may use assumptions that may not hold in real datasets.

9

MRHC Problem

Find a minimum recombinant haplotype configuration from a given pedigree with genotype data.

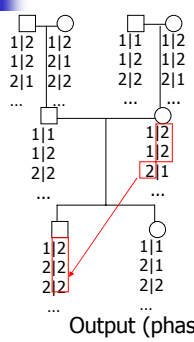
Assumptions:
- Mendelian law (no mutations)
- Recombination events are **rare**



Input (phase unknown)

10

The MRHC Problem



- PS: parental source of the two alleles at the locus (*i.e.* phase)
- Haplotype configuration = assignment of PS values at each locus of every individual.

PS = 1 (because the allele with the smaller index is maternal)

Output (phase known)

11

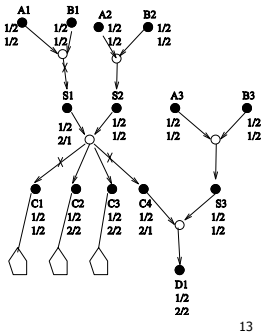
Previous Results

- Genotype elimination (O'Connell & Weeks'99).
  - Can only find haplotype configurations requiring no recombinant in the pedigree, exhaustive elimination.
- Genetic algorithm (Tapadar *et al.*'00).
  - Still time consuming, needs many iterations before convergence.
- MRH (Qian & Beckmann'02).
  - Six step rule-based algorithm.
  - Locus by locus at every step, extremely slow for biallelic (*e.g.* SNP) markers.

12

Thm. MRHC is NP-hard.

- Idea: Reduction from a variant of set cover.
- First complexity result concerning the problem.
- Remains hard when there are only two loci.
- Remains hard when no loops in a pedigree.



13

An Exact Algorithm for 0-Recombinant Data Based on Resolution of Constraints

- Assumptions:
  - Zero recombinants.
  - No missing alleles, no errors.
- Idea: finding all feasible (*i.e.* 0-recombinant) haplotype configurations is equivalent to reducing the degree of freedom in PS assignment.
- Steps:
  - formulate all the constraints, as linear equations over GF(2)
  - solve the equations by Gaussian elimination
  - enumerate all feasible haplotype configurations

14

Four Levels of Constraints

Based on Mendelian law (for single locus) :

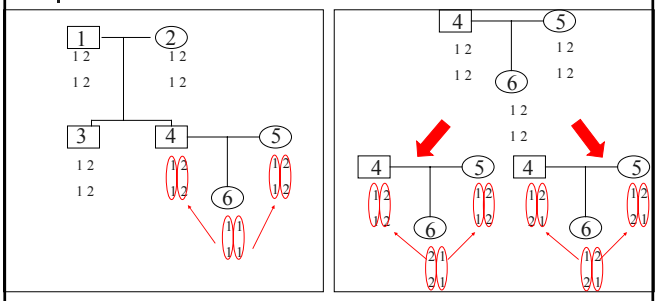
- Level 1: GS (grantparental source) constraint
- Level 2: PS constraint

Based on 0-recombinant assumption (for a pair of loci):

- Level 3: Haplotype constraint
- Level 4: Grouping constraint

15

Level 3 and Level 4 Constraints



16

Level 3 and level 4 Constraints

	x	y	z	Constraint equations
1	1 2 / 1 2	1 ∗ / 1 ∗	1 1 / 1 1	$x_1 = x_2$
2	1 2 / 2 1	1 ∗ / 2 ∗	1 1 / 2 2	$x_1 + x_2 = 1$
3	1 2 / 2 1	1 ∗ / 1 1	1 1 / 2 1	$x_1 + x_2 = 1$
4	1 2 / 1 2	1 1 / 1 1	2 1 / 2 1	$x_1 = x_2$

Table 1: The possible level 3 constraints.

	x	y	z	Constraint equations
1	1 2 / 1 2	1 2 / 1 2	1 2 / 1 2	$x_1 + x_2 = y_1 + y_2 = z_1 + z_2$
2	1 2 / 1 2	1 2 / 2 1	1 2 / 1 1	$x_1 + x_2 = z_1, y_1 + y_2 + z_1 = 1$
3	1 2 / 1 2	1 2 / 1 1	2 1 / 2 1	$x_1 + x_2 = z_1 + z_2$

Table 2: The possible level 4 constraints.

Note: The variables represent PS values and the equations are over GF(2) (in fact, addition mod 2).

17

Constraint-Based Algorithm

Thm. Every solution consistent with the constraint equations is a feasible solution and vice versa.

We can adapt the classical Gaussian elimination algorithm to find all consistent solutions in $O(n^3m^3)$ time.

Previously, only an exponential time algorithm is known due to O'Connell and Weeks (1999).

The algorithm is useful for solving 0-recombinant data and may serve as a subroutine in a general haplotyping algorithm.

18

Block-Extension Algorithm

Iterative, heuristic, five steps. Rules are derived from Mendelian law, MR principle, block concept and some greedy ideas based on the following observations:

- Block structures are common in haplotypes.
- Double recombination events are rare.
- Common haplotype blocks shared in siblings.
- …

19

Steps in the BE algorithm

- Missing allele imputation by the Mendelian Law of inheritance and allele frequency
- PS assignment by Mendelian Law
  - Locus by locus, member by member, in a top-down scan
- Greedy assignment of PS
  - Bottom-up, infer PS value from PS of adjacent loci.
- Block-Extension
  - Iteratively extend the longest block to the same region of other members.
- Finishing the gaps between blocks by enumeration.

20

Analysis of the BE Algorithm

- Advantage:
  - Simple and efficient.
  - Accurate when the number of recombination events is small.
- Disadvantage:
  - Potential errors in steps 3 and 4. Accuracy could decrease with the increase of the number of recombination events.

21

More Exact Algorithms

- Locus-based dynamic programming algorithm
  - Linear time in the number of the members
  - Applicable to only tree pedigrees
- Member-based dynamic programming algorithm
  - Linear time in the number of the loci
  - Applicable to general pedigrees with small size
- Integer linear programming (ILP) with branch-and-bound
  - Combines missing data imputation and haplotype inference together.
  - It also implicitly checks Mendelian consistency for pedigree genotype data with missing alleles, which is also an NPC problem.
  - Effective for practical size problems, regardless of the pedigree structure

22

ILP for MRHC with Missing Data

1. Alleles are represented as binary variables.
2. Genotype info and the Mendelian law of inheritance are enforced by linear constraints.
3. The objective of minimizing the total number of recombinants is encoded as a linear function of the variables.
4. Effective preprocessing of constraints by taking advantage of special properties in our ILP formulation to reduce the number of variables.
5. Branch-and-bound strategy to find solutions. The branch step guided by a partial order relationship (and some other special relationships) identified during the preprocessing step.
6. Non-trivial bounds are estimated to prune the search tree.
7. A maximum likelihood approach is used to select the best haplotype configuration from multiple optimal solutions.

23

Formulation: variables

- Possible alleles (totally t_j) at marker locus j: $M_j = \{m_1^j, \ldots, m_{t_j}^j\}$
- Define $2t_j$ (f and m) vars and 2 g vars for each paternal allele and maternal allele at locus j for individual i

  $f_{i,k}^j, m_{i,k}^j \ (1 \le k \le t_j) \quad g_{i,1}^j, g_{i,2}^j$
- Var f_k (or m_k)=1 iff the allele is m_k. Var g_1 = 0 (or 1) iff paternal allele is copied from father's paternal (or maternal) allele. Var g_2 defined similarly.
- Define r vars:

  $r_{i,1}^j, r_{i,2}^j \ (1 \le j \le m-1)$

  $r_{i,1}^j = 1 \text{ iff } g_{i,1}^j \ne g_{i,1}^{j+1}$

24

Formulation

- Objective function:

$$\sum_{\text{Non-Founders}} \sum_{j=1}^{m-1} (r_{i,1}^j + r_{i,2}^j)$$

Subject to

Genotype constraints: (0 means missing allele)

$$\{0,0\} \Rightarrow \{\sum_{k=1}^{t_f} f_{i,k}^j = 1, \sum_{k=1}^{t_f} m_{i,k}^j = 1\}$$

$$\{m_r^j, 0\} \Rightarrow \{f_{i,r}^j + m_{i,r}^j \geq 1\}$$

$$\{m_r^j, m_r^j\} \Rightarrow \{f_{i,r}^j = m_{i,r}^j = 1\}$$

$$\{m_r^j, m_s^j\} \Rightarrow \{f_{i,r}^j + f_{i,s}^j = m_{i,r}^j + m_{i,s}^j = f_{i,r}^j + m_{i,r}^j = f_{i,s}^j + m_{i,s}^j = 1\}$$

Formulation

- Mendelian law of inheritance constraints (for a child *i* and its father *f*):

$$f_{i,k}^j - f_{f,k}^j - g_{i,1}^j \leq 0$$

$$f_{i,k}^j - m_{f,k}^j + g_{i,1}^j \leq 1$$

- Constraints for *r* vars:

$$r_{i,l}^j - g_{i,l}^j - g_{i,l}^{j+1} \leq 0$$

$$r_{i,l}^j + g_{i,l}^j + g_{i,l}^{j+1} \leq 2$$

$$-r_{i,l}^j + g_{i,l}^j - g_{i,l}^{j+1} \leq 0$$

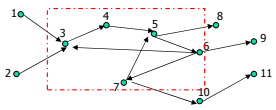
$$-r_{i,l}^j - g_{i,l}^j + g_{i,l}^{j+1} \leq 0$$

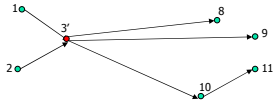
A Partial Order Relationship

Denote: $y^\gamma = \begin{cases} y & \gamma = 1 \\ 1 - y & \gamma = 0 \end{cases}$

Inequalities with 2 variables:

$$y_i^\alpha \leq y_j^\beta$$





Forced Variables

- Rule 1: $y^0, y^1 \in S \Rightarrow \text{Inconsistency}$
- Rule 2: $(y_i^\alpha \leq y_j^\beta) \wedge (y_i^\alpha \leq y_j^{1-\beta}) \Rightarrow y_i^\alpha = 0$

  $(y_i^\alpha \leq y_j^\beta) \wedge (y_i^{1-\alpha} \leq y_j^\beta) \Rightarrow y_j^\beta = 1$
- Rule 3: $y_i^\alpha \leq y_i^{1-\alpha} \Rightarrow y_i^\alpha = 0$

Lower and Upper Bounds

- Lower bounds
  - Linear relaxation.
  - Sum of minimum number of recombinants in each nuclear family.
  - Effective for data with a large number of recombinants.
- Upper bound
  - Obtained by the Block-Extension algorithm.
  - Effective for data with a small number of recombinants.

ILP

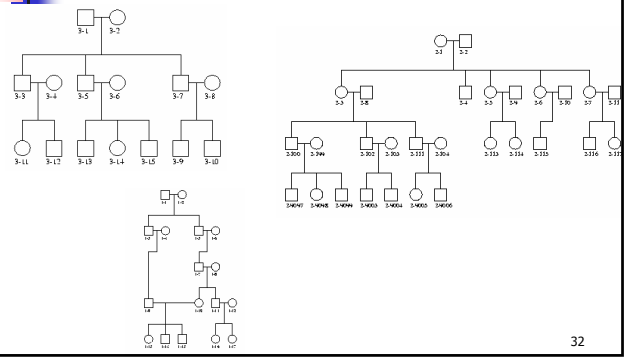
- Practical in terms of time efficiency
- Could find all possible optimal solutions
- Very effective in terms of missing allele imputation.

Simulation Studies

- The algorithms have been implemented in a program called PedPhase in C++.
- Simulated data were generated to compare our algorithms, and with MRH (Qian&Beckmann'02)
- Three different pedigree structures.
- Multiallelic and biallelic data.
- Numbers of loci: 10, 25 and 50.
- Number of recombinants: 0-4.
- 100 runs per data set.

31

Pedigree Structures



32

Accuracy Results of Algrotihm Block-Extension

Parameters	Results
(15,50,6,0)	100
(15,50,6,4)	91
(17,50,6,0)	100
(17,50,6,4)	91
(29,10,6,0)	100
(29,10,6,4)	99
(29,25,6,0)	100
(29,25,6,4)	95
(29,50,6,0)	100
(29,50,6,1)	96
(29,50,6,2)	93
(29,50,6,3)	95
(29,50,6,4)	91

Parameters	Results
(15,50,2,0)	100
(15,50,2,1)	82
(17,25,2,0)	100
(17,25,2,1)	84
(17,50,2,0)	100
(17,50,2,1)	72
(29,10,2,0)	95
(29,10,2,4)	93
(29,25,2,0)	100
(29,25,2,1)	91
(29,25,2,2)	87
(29,50,2,0)	100
(29,50,2,1)	88

Table 5: Percentages correctly recovered out of 100 runs by the block-extension algorithm on multi-allelic (left) and biallelic (right) markers.

33

Efficiency Results

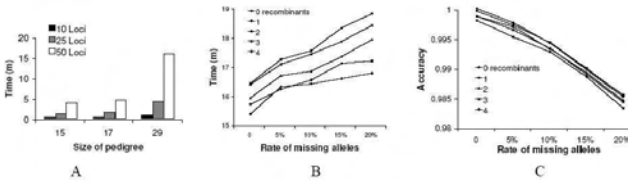
Table 1: Speeds of BE, MRH and ILP on multi-allelic (left) and biallelic (right) markers.

Parameters	Time used by BE	Time used by MRH	Time used by ILP
(17,10,6,0)	2.1s	7s	34s
(17,10,6,4)	2.1s	11s	37s
(15,25,6,0)	2.7s	18s	2m34s
(15,25,6,4)	2.9s	33s	3m9s
(29,10,6,0)	3.2s	10s	1m49s
(29,10,6,4)	3.1s	15s	1m57s
(29,25,6,0)	15s	4m	15m2s
(29,25,6,4)	10s	2m6s	15m10s

Parameters	Time used by BE	Time used by MRH	Time used by ILP
(17,10,2,0)	1.9s	15s	20s
(17,10,2,4)	2.3s	1m11s	23s
(15,25,2,0)	4.7s	10m50s	1m6s
(15,25,2,4)	4.8s	13m49s	1m18s
(29,10,2,0)	2.8s	6m26s	44s
(29,10,2,4)	2.7s	3m46s	50s
(29,25,2,0)	2.3s	2h7m	3m41s
(29,50,2,0)	16s	45h	15m21s

34

More Results on ILP



A B C

Figure 4: Some simulation results on ILP. A. Effect of problem size on speed. B. Effect of number of recombinants and rate of missing alleles on speed. C. Effect of number of recombinants and rate of missing alleles on accuracy.

35

Real Data Analysis

- Data set (Gabriel *et al.*'02)
  - 93 members, 12 pedigrees (each with 7-8 members);
  - chromosome 3, 4 regions, each region 1-4 blocks.

Region name	Physical length (kbps)	Genotyped SNPs	Block	SNPs in each block
16a	40	14	1	5
16b	106	53	1	6
			2	4
17a	186	70	1	6
			2	5
			3	4
			4	6
18a	286	74	1	16
			2	6
			3	4

Table 8: The regions and blocks on chromosome 3.

Reconstruction of Common Haplotypes and Estimation of Their Frequencies

Table 4: Common haplotypes and their frequencies obtained by block-extension, ILP and the EM method. In haplotypes, the alleles are encoded as 1=A, 2=C, 3=G, and 4=T.

Block	EM		Block-extension		ILP	
	Common haplotypes	Frequencies	Common haplotypes	Frequencies	Common haplotypes	Frequencies
16a-1	4 2 2 2 2	0.4232	4 2 2 2 2	0.3817	4 2 2 2 2	0.3750
	3 4 3 4 4	0.2187	3 4 3 4 4	0.1720	3 4 3 4 4	0.2187
	4 2 2 2 4	0.2018	4 2 2 2 4	0.1935	4 2 2 2 4	0.1979
	3 4 2 2 4	0.1432	3 4 2 2 4	0.1613	3 4 2 2 4	0.1458
sum		0.9869		0.9085		0.9374
16b-1	3 2 4 1 1 2	0.8014	3 2 4 1 1 2	0.7634	3 2 4 1 1 2	0.7813
	1 3 2 3 3 4	0.0833	1 3 2 3 3 4	0.0753	1 3 2 3 3 4	0.0833
sum		0.8847		0.8387		0.8646
16b-2	4 1 2 2	0.5410	4 1 2 2	0.4892	4 1 2 2	0.5104
	2 3 3 4	0.2812	2 3 3 4	0.2581	2 3 3 4	0.2500
	2 3 3 2	0.1562	2 3 3 2	0.1344	2 3 3 2	0.1562
sum		0.9784		0.8788		0.9166
17a-1	3 1 3 4 4 4	0.3403	3 1 3 4 4 4	0.3172	3 1 3 4 4 4	0.2917
	1 3 3 2 4 2	0.3021	1 3 3 2 4 2	0.2419	1 3 3 2 4 2	0.2500
	3 3 2 4 2 4	0.1354	3 3 2 4 2 4	0.0914	3 3 2 4 2 4	0.0938
	3 3 3 4 4 4	0.1021	3 3 3 4 4 4	0.1183	3 3 3 4 4 4	0.1354
	3 3 2 4 4 4	0.0681	3 3 2 4 4 4	0.0806	3 3 2 4 4 4	0.0729
	1 3 3 2 4 4	0.0521				
sum		1.0000		0.8494		0.8438
17a-2	2 3 2 4 2	0.3542	2 3 2 4 2	0.2903	2 3 2 4 2	0.3229
	3 3 4 2 4	0.3333	3 3 4 2 4	0.2957	3 3 4 2 4	0.3125
	3 3 4 4 2	0.1458	3 3 4 4 2	0.1344	3 3 4 4 2	0.1563
	3 4 4 4 4	0.1250	3 4 4 4 4	0.1452	3 4 4 4 4	0.1250
sum		0.9583		0.8656		0.9167

Results from ILP on the Whole Dataset

Table 2: Comparison of the EM and ILP algorithms on a human genome SNP data.

Chromosome	# of blocks	Ave # of common haplotypes by EM	Ave # of common haplotypes by ILP	Ave # of differences between EM and ILP	Ave # of recombinants by ILP
1	22	3.82	4.00	0.45	0.034
2	6	3.33	4.00	0.67	0.000
3	10	3.9	4.00	0.50	0.033
4	7	3.57	3.29	0.14	0.048
5	7	3.86	4.12	0.43	0.024
6	11	3.55	3.54	0.67	0.008
7	9	2.67	3.33	0.22	0.037
8	8	3.63	3.38	0.25	0.000
9	3	3.67	4.33	1.33	0.333
10	7	4.14	3.57	0.71	0.095
11	5	3.40	3.60	0.40	0.083
12	6	3.00	2.83	0.17	0.00
13	6	3.67	3.83	0.50	0.042
14	4	3.50	3.50	0.00	0.000
15	3	3.33	4.33	1.00	0.028
16	4	3.50	3.75	0.25	0.125
17	2	2.5	2.00	0.50	0.000
18	4	3.25	3.25	0.25	0.125
20	2	4.00	4.00	0.00	0.000
21	1	2.00	3.00	1.00	0.167
22	8	4.12	3.88	0.50	0.021

38

Application of Haplotype Inference in Gene Association Mapping

- We have developed a new haplotype association mapping method based on density-based clustering for case-control data.
- The method regards haplotype segments as data points in a high dimensional space, and defines a new pairwise haplotype distance measure.
- Clusters are then identified by a density-based clustering algorithm.
- *Z*-scores based on the number of cases and controls in a cluster can be used as an indicator of the degree of association between a cluster and the disease under study.
- Results are very promising.
- But it needs haplotypes as input.

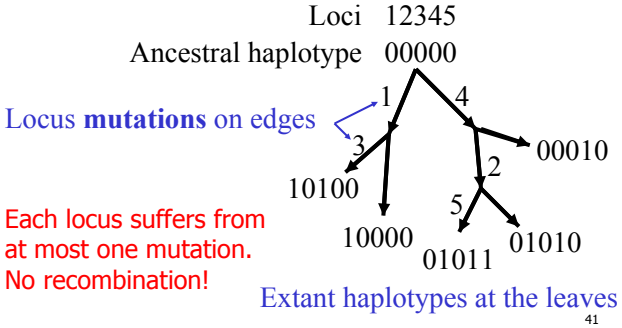
39

An Application of Haplotype Inference

- Haplotypes are inferred by computational methods that we mentioned earlier.
- For example: a real data set that we analyzed consists of 385 nuclear families of size 4 (2 parents with 2 affected children).
- We do haplotype inference first using our ILP algorithm. The haplotypes transmitted to (affected) children are treated as cases and un-transmitted haplotypes as controls. The haplotype association method was applied then.

40

Inference of Haplotypes from Population Data: The Perfect Phylogeny Model



41

Perfect Phylogeny Haplotype (PPH)

Given a set/poplation of genotypes S, find an explanatory set of haplotypes that fits a perfect phylogeny.

S	Loci 1	2
a	2	2
b	0	2
c	1	0

Genotype matrix

The genotype coding:
(11): 0 homozygous
(22): 1 homozygous
(12): 2 heterozygous

A haplotype pair explains a genotype if the merge of the haplotypes creates the genotype. E.g., merging haplotypes 001 and 100 results in genotype 202.

42

Perfect Phylogeny Haplotype (PPH)

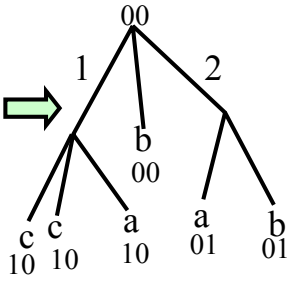
Given a set of genotypes S, find an explanatory set of haplotypes that fits a perfect phylogeny.

	1	2
a	2	2
b	0	2
c	1	0

⇒

	1	2
a	1	0
a	0	1
b	0	0
b	0	1
c	1	0
c	1	0

⇒



An Alternative Haplotype Explanation

	1	2
a	2	2
b	0	2
c	1	0

⇒

	1	2
a	1	1
a	0	0
b	0	0
b	0	1
c	1	0
c	1	0

⇒ No perfect phylogeny exists for this explanation

Efficient Solutions to the PPH Problem with n Individuals and m Loci

- Reduction to a graph realization problem (GPPH), based on Bixby-Wagner or Fushishige solution to graph realization (Gusfield'01).
- Reduction to graph realization, based on Tutte's graph realization method, in O(nm^2) time (Gusfield'02).
- Direct combinatorial approach in O(nm^2) time. Bafna *et al.*'03
- Eskin, Halperin and Karp'03: Specialize the Tutte solution to the PPH problem, in O(nm^2) time.

Summary

- Li, J. and T. Jiang. Efficient Rule-Based Haplotyping Algorithm for Pedigree Data. *RECOMB'03*
  - NP-completeness proof for general pedigrees.
  - An efficient heuristic algorithm: block-extension.
  - An efficient exact algorithm for 0-recombinant data.
- Doi, K., J. Li and T. Jiang. Minimum Recombinant Haplotype Configuration on Tree Pedigrees. *WABI'03*
  - NP-completeness proof for loopless (or tree) pedigrees.
  - Two dynamic programming algorithms
- Li, J. and T. Jiang. An Exact Solution for Finding Minimum Recombinant Haplotype Configurations on Pedigrees with Missing Data by Integer Linear Programming. *RECOMB'04.*
- Li, J. and T. Jiang. Haplotype Association Mapping by Density-Based Clustering in Case-Control Studies. *RECOMB Satellite Workshop on Computational Methods for SNPs and Haplotypes*, CMU, 2004.

Future Work

- Incorporating mutations and errors into MRHC.
- Incorporating the likelihood of recombination into the objective function of ILP.
- Haplotype inference and missing allele imputation without pedigree information.
- Approximation algorithms for MRHC, especially MRHC on tree pedigrees.
- Efficient fixed-parameter (# of recombinants) algorithms.

Acknowledgements

Dr. Dajun Qian from City of Hope.

Whitehead/MIT Center for Genome Research
Drs. David Altshuler, Mark Daly, Stacey Gabriel, and Stephen Schaffner, and their entire group.

Financial support from NSF and CMOST 973 project.

New Horizons in Machine Learning

Avrim Blum CMU

This is mostly a survey, but portions near the end are joint work with Nina Balcan and Santosh Vempala

[Workshop on New Horizons in Computing, Kyoto 2005]

What is Machine Learning?

- Design of programs that adapt from experience, identify patterns in data.
- Used to:
  - recognize speech, faces, images
  - steer a car,
  - play games,
  - categorize documents, info retrieval, ...
- Goals of ML theory: develop models, analyze algorithmic and statistical issues involved.

Plan for this talk

- Discuss some of current challenges and "hot topics".
- Focus on topic of "kernel methods", and connections to random projection, embeddings.
- Start with a quick orientation...

The concept learning setting

- Imagine you want a computer program to help you decide which email messages are spam and which are important.
- Might represent each message by n features. (e.g., return address, keywords, spelling, etc.)
- Take sample S of data, labeled according to whether they were/weren't spam.
- Goal of algorithm is to use data seen so far to produce good prediction rule (a "hypothesis") h(x) for future data.

The concept learning setting

E.g.,

money	pills	Mr.	bad spelling	known-sender	spam?
Y	N	Y	Y	N	Y
N	N	N	Y	Y	N
N	Y	N	N	N	Y
Y	N	N	N	Y	N
N	N	Y	N	Y	N
Y	N	N	Y	N	Y
N	N	Y	N	N	N
N	Y	N	Y	N	Y

example *label*

Given data, some reasonable rules might be:

- Predict SPAM if unknown AND (money OR pills)
- Predict SPAM if money + pills – known > 0.
- ...

Big questions

(A) How to optimize?

- How might we automatically generate rules like this that do well on observed data? [Algorithm design]

(B) What to optimize?

- Our real goal is to do well on new data.
- What kind of confidence do we have that rules that do well on sample will do well in the future?
  - Statistics
  - Sample complexity
  - SRM

for a given learning alg, how much data do we need...

To be a little more formal…

PAC model setup:

- Alg is given sample $S = \{(x,l)\}$ drawn from some distribution D over examples x, labeled by some target function f.
- Alg does optimization over S to produce some hypothesis $h \in H$. [e.g., H = linear separators]
- Goal is for h to be close to f over D.
  - $Pr_{x \in D}(h(x) \neq f(x)) \leq \varepsilon$.
- Allow failure with small prob δ (to allow for chance that S is not representative).

The issue of sample-complexity

- We want to do well on D, but all we have is S.
  - Are we in trouble?
  - How big does S have to be so that low error on S $\Rightarrow$ low error on D?
- Luckily, simple sample-complexity bounds:
  - If $|S| \geq (1/\varepsilon)[\log|H| + \log 1/\delta]$,
    [think of log|H| as the number of bits to write down h]
    then whp $(1-\delta)$, all $h \in H$ that agree with S have true error $\leq \varepsilon$.
  - In fact, with extra factor of $O(1/\varepsilon)$, enough so whp all have |true error – empirical error| $\leq \varepsilon$.

The issue of sample-complexity

- We want to do well on D, but all we have is S.
  - Are we in trouble?
  - How big does S have to be so that low error on S $\Rightarrow$ low error on D?
- Implication:
  - If we view cost of examples as comparable to cost of computation, then don't have to worry about data cost since just ~ $1/\varepsilon$ per bit output.
  - But, in practice, costs often wildly different, so sample-complexity issues are crucial.

Some current hot topics in ML

- More precise confidence bounds, as a function of observable quantities.
  - Replace log |H| with log(# ways of splitting S using functions in H).
  - Bounds based on margins: how well-separated the data is.
  - Bounds based on other observable properties of S and relation of S to H; other complexity measures…

Some current hot topics in ML

- More precise confidence bounds, as a function of observable quantities.
- Kernel methods.
  - Allow to implicitly map data into higher-dimensional space, without paying for it if algorithm can be "kernelized".
  - Get back to this in a few minutes…
  - Point is: if, say, data not linearly separable in original space, it could be in new space.

Some current hot topics in ML

- More precise confidence bounds, as a function of observable quantities.
- Kernel methods.
- Semi-supervised learning.
  - Using labeled and unlabeled data together (often unlabeled data is much more plentiful).
  - Useful if have beliefs about not just form of target but also its relationship to underlying distribution.
  - Co-training, graph-based methods, transductive SVM,…

Some current hot topics in ML

- More precise confidence bounds, as a function of observable quantities.
- Kernel methods.
- Semi-supervised learning.
- Online learning / adaptive game playing.
  - Classic strategies with excellent regret bounds (from Hannan in 1950s to weighted-majority in 80s-90s).
  - New work on strategies that can efficiently handle large implicit choice spaces. [KV][Z]…
  - Connections to game-theoretic equilibria.

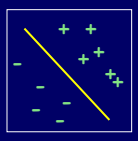
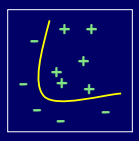
Some current hot topics in ML

- More precise confidence bounds, as a function of observable quantities.
- Kernel methods.
- Semi-supervised learning.
- Online learning / adaptive game playing.

Could give full talk on any one of these.
Focus on #2, with connection to random projection and metric embeddings…

Kernel Methods

- One of the most natural approaches to learning is to try to learn a linear separator.

- But what if the data is not linearly separable? Yet you still want to use the same algorithm.
- One idea: Kernel functions.

Kernel Methods

- A Kernel Function $K(x,y)$ is a function on pairs of examples, such that for some implicit function $\Phi(x)$ into a possibly high-dimensional space, $K(x,y) = \Phi(x) \cdot \Phi(y)$.
- E.g., $K(x,y) = (1 + x \cdot y)^m$.
  - If $x \in R^n$, then $\Phi(x) \in R^{n^m}$.
  - K is easy to compute, even though you can't even efficiently write down $\Phi(x)$.
- The point: many linear-separator algorithms can be *kernelized* – made to use K and act *as if* their input was the $\Phi(x)$'s.
  - E.g., Perceptron, SVM.

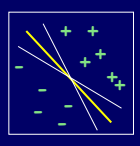
Typical application for Kernels

- Given a set of images: , represented as pixels, want to distinguish men from women.
- But pixels not a great representation for image classification.
- Use a Kernel K(,) = Φ( )·Φ( ), Φ is implicit, high-dimensional mapping. Choose K appropriate for type of data.

What about sample-complexity?

- Use a Kernel K(,) = Φ( )·Φ( ), Φ is implicit, high-dimensional mapping.
- What about # of samples needed?
  - Don't have to pay for dimensionality of Φ-space if data is separable by a large margin γ.
  - E.g., Perceptron, SVM need sample size only $\tilde{O}(1/\gamma^2)$.

$|w \cdot \Phi(x)| / |\Phi(x)| \geq \gamma, \quad |w|=1$



So, with that background…

Question

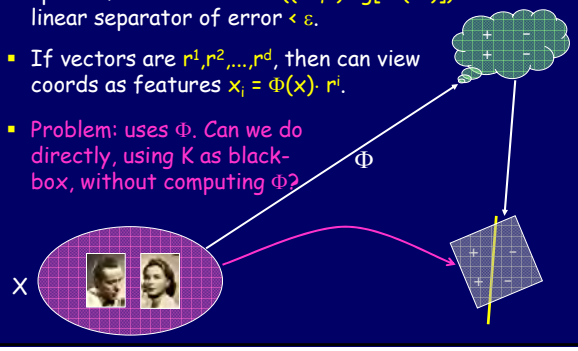
- Are kernels really allowing you to magically use power of implicit high-dimensional Φ-space without paying for it?
- What's going on?
- Claim: [BBV] Given a kernel [as a black-box program K(x,y)] and access to typical inputs [samples from D],
  - Can run K and reverse-engineer an explicit (small) set of features, such that if K is good [∃ large-margin separator in Φ-space for f,D], then this is a good feature set [∃ almost-as-good separator in this explicit space].

contd

- Claim: [BBV] Given a kernel [as a black-box program K(x,y)] & access to typical inputs [samples from D]
  - Can run K and reverse-engineer an explicit (small) set of features, such that if K is good [∃ large-margin separator in Φ-space], then this is a good feature set [∃ almost-as-good separator in this explicit space].
- Eg, sample $z^1,\ldots,z^d$ from D. Given x, define $x_i=K(x,z^i)$.
- Implications:
  - Practical: alternative to kernelizing the algorithm.
  - Conceptual: View choosing a kernel like choosing a (distrib dependent) set of features, rather than "magic power of implicit high dimensional space". [though argument needs existence of Φ functions]

Why is this a plausible goal in principle?

- JL lemma: If data separable with margin γ in Φ-space, then with prob $1-\delta$, a *random* linear projection down to space of dimension $d = O((1/\gamma^2)\log[1/(\delta\varepsilon)])$ will have a linear separator of error $< \varepsilon$.
- If vectors are $r^1,r^2,\ldots,r^d$, then can view coords as features $x_i = \Phi(x)\cdot r^i$.
- Problem: uses Φ. Can we do directly, using K as black-box, without computing Φ?



3 methods (from simplest to best)

1. Draw d examples $z^1,\ldots,z^d$ from D. Use:
   $F(x) = (K(x,z^1), \ldots, K(x,z^d))$. [So, "$x_i$" = $K(x,z^i)$]

   For $d = (8/\varepsilon)[1/\gamma^2 + \ln 1/\delta]$, if separable with margin γ in Φ-space, then whp this will be separable with error ε. (but this method doesn't preserve margin).

2. Same d, but a little more complicated. Separable with error ε at margin $\gamma/2$.

3. Combine (2) with further projection as in JL lemma. Get d with log dependence on $1/\varepsilon$, rather than linear. So, can set $\varepsilon \ll 1/d$.

All these methods need access to D, unlike JL. Can this be removed? We show **NO** for generic K, but may be possible for natural K.

Actually, the argument is pretty easy…

(though we did try a lot of things first that didn't work…)

Key fact

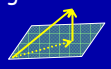
Claim: If $\exists$ perfect w of margin γ in ϕ-space, then if draw $z^1,\ldots,z^d \in D$ for $d \geq (8/\varepsilon)[1/\gamma^2 + \ln 1/\delta]$, whp $(1-\delta)$ exists w' in span$(\Phi(z^1),\ldots,\Phi(z^d))$ of error $\leq \varepsilon$ at margin $\gamma/2$.

Proof: Let S = examples drawn so far. Assume $|w|=1$, $|\Phi(z)|=1\ \forall\ z$.

- w_{in} = proj(w,span(S)), $w_{out} = w - w_{in}$.
- Say w_{out} is **large** if $\Pr_z(|w_{out}\cdot\Phi(z)| \geq \gamma/2) \geq \varepsilon$; else **small**.
- If small, then done: $w' = w_{in}$.
- Else, next z has at least ε prob of improving S.

$$|w_{out}|^2 \leftarrow |w_{out}|^2 - (\gamma/2)^2$$

- Can happen at most $4/\gamma^2$ times. □



So....

If draw $z^1,\ldots,z^d \in D$ for $d = (8/\varepsilon)[1/\gamma^2 + \ln 1/\delta]$, then whp exists w' in span$(\Phi(z^1),\ldots,\Phi(z^d))$ of error $\leq \varepsilon$ at margin $\gamma/2$.

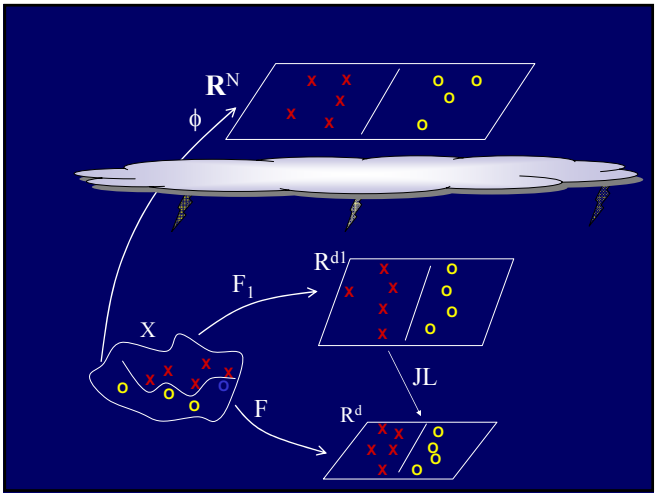
- So, for some $w' = \alpha_1\Phi(z^1) + \ldots + \alpha_d\Phi(z^d)$,
  $\Pr_{(x,l)\in P}[\text{sign}(w'\cdot\Phi(x)) \neq l] \leq \varepsilon$.
- But notice that $w'\cdot\Phi(x) = \alpha_1K(x,z^1) + \ldots + \alpha_dK(x,z^d)$.
  $\Rightarrow$ vector $(\alpha_1,\ldots\alpha_d)$ is an ε-good separator in the feature space: $x_i = K(x,z^i)$.
- But margin not preserved because length of target, examples not preserved.

What if we want to preserve margin? (mapping 2)

- Problem with last mapping is $\Phi(z)$'s might be highly correlated. So, dot-product mapping doesn't preserve margin.
- Instead, given a new x, want to do an orthogonal projection of $\Phi(x)$ into that span. (preserves dot-product, decreases $|\Phi(x)|$, so only increases margin).
  - Run $K(z^i,z^j)$ for all i,j=1,...,d. Get matrix M.
  - Decompose $M = U^TU$.
  - (Mapping #2) = (mapping #1)U^{-1}. □

Use this to improve dimension

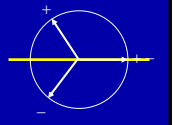
- Current mapping gives $d = (8/\varepsilon)[1/\gamma^2 + \ln 1/\delta]$.
- Johnson-Lindenstrauss gives $d = O((1/\gamma^2)\log 1/(\delta\varepsilon))$. Nice because can have $d \ll 1/\varepsilon$. [So can set ε small enough so that whp a sample of size O(d) is perfectly separable]
- Can we achieve that efficiently?
- Answer: just combine the two...
  - Run Mapping #2, then do random projection down from that. (using fact that mapping #2 had a margin)
  - Gives us desired dimension (# features), though sample-complexity remains as in mapping #2.



Lower bound (on necessity of access to D)

For **arbitrary** black-box kernel K, can't hope to convert to small feature space without access to D.

- Consider $X=\{0,1\}^n$, random $X' \subset X$ of size $2^{n/2}$, D = uniform over X'.
- c = arbitrary function (so learning is hopeless).
- But we have this magic kernel $K(x,y) = \Phi(x)\cdot\Phi(y)$
  - $\Phi(x) = (1,0)$ if $x \notin X'$.
  - $\Phi(x) = (-\frac{1}{2}, \sqrt{3}/2)$ if $x \in X'$, c(x)=pos.
  - $\Phi(x) = (-\frac{1}{2}, -\sqrt{3}/2)$ if $x \in X'$, c(x)=neg.
- P is separable with margin $\sqrt{3}/2$ in Φ-space.
- But, without access to D, all attempts at running $K(x,y)$ will give answer of 1.



Open Problems

- For specific natural kernels, like "polynomial" kernel $K(x,y) = (1 + x \cdot y)^m$, is there an efficient analog to JL, without needing access to D?
  - Or, can one at least reduce the sample-complexity ? (use fewer accesses to D)
  - This would increase practicality of this approach
- Can one extend results (e.g., mapping #1: $x \rightarrow [K(x,z^1), ..., K(x,z^d)]$) to more general similarity functions K?
  - Not exactly clear what theorem statement would look like.

Rigorous analysis of heuristics for NP-hard problems

Uriel Feige
Weizmann Institute
Microsoft Research

1

Computational problems

We would love to have algorithms that:

- Produce optimal results.
- Are efficient (polynomial time).
- Work on every input instance.

2

NP-hardness

For many combinatorial problems, the goal of achieving all three properties simultaneously is too ambitious (NP-hard).

We should set goals that are more modest.

3

Relaxing the desired properties

Optimality: approximation algorithms.

Efficiency: sub-exponential algorithms, fixed parameter tractability.

Firm theoretical foundations. Both positive and negative results.

4

Heuristics

Relax the universality property: need not work on every input.

In this talk: heuristics are required to produce optimal results in polynomial time, on typical inputs.

Conceptual problem: the notion typical is not well defined.

5

Some questions

Explain apparent success of known heuristics.
Come up with good heuristic ideas.
Match heuristics to problems.
Investigate fundamental limitations.

Prove that a certain heuristic is good.
Prove that a certain heuristic is bad.

6

In this talk

Some theoretical frameworks for studying heuristics.

Some algorithmic ideas that are often used.

Heuristics is a huge subject. This talk presents only a narrow view, and excludes many important and relevant work.

7

The importance of modeling

For a rigorous treatment of heuristics, need a rigorous definition for typical inputs.

Given a rigorous definition for typical inputs (for example, planar graphs), one is no longer dealing with a fuzzy notion of heuristics, but rather with the familiar notion of worst case analysis.

8

Probabilistic models

A typical input can be modeled as a random input chosen from some well defined distribution on inputs.

Again, design of heuristics often boils down to worst case analysis:

- Most random inputs have property P.
- Algorithm works on all inputs with property P.

9

Rigorous analysis

In this talk, limit ourselves to discussion of heuristics in well defined models. In these models, prove theorems.

To early to assess the relevance and success of the methodology.

10

Some theoretical frameworks

Random inputs.

Planted solution models.

Semi-random models, monotone adversary.

Smoothed analysis.

Stable inputs.

11

Random inputs

Typical example: random graphs, n vertices, m edges.

An algorithm for finding Hamiltonian cycles in random graphs, even when the minimum degree is 2 [Bollobas,Fenner,Frieze].

No algorithm known for max clique in random graphs.

12

Planted solution models

Useful when random model seems too difficult.

Example: plant in a uniform random graph a clique of large size k. Can a polynomial time algorithm find the k-clique?

- Yes, when $k = \Omega(\sqrt{n})$ [Alon,Krivelevich,Sudakov].
- Unknown when $k = o(\sqrt{n})$.

13

Semi random model [Blum-Spencer]

Useful in order to overcome over-fitting of algorithms to the random model. Adds robustness to algorithms.

Example, when $k >> \sqrt{n \log n}$, vertices of planted k-clique have highest degree.

Algorithm may select the k highest degree vertices and check if they form a clique.

14

Monotone adversary [Feige-Kilian]

Adversary may change the random input, but only in one direction.

Planted clique: adversary may remove arbitrarily many non-clique edges.

Degree based algorithm no longer works.

Semidefinite programming does work, when $k = \Omega(\sqrt{n})$ [Feige-Krauthgamer].

15

Smoothed analysis [Spielman-Teng]

Arbitrary input, random perturbation.

Typical input – low order bits are random.

Explain success of simplex algorithm [ST].

FPTAS implies easy smoothed instances [Beier-Voecking].

16

Smoothed versus semirandom

Smoothed analysis:
- arbitrary instance – defines an arbitrary region.
- random input is chosen in this region.
- stronger when region is small.

Monotone adversary:
- random instance – defines a random region.
- arbitrary input is chosen in region.
- stronger when region is large.

17

Stable inputs [Bilu-Linial]

In some applications (clustering), the interesting inputs are those that are stable in the sense that a small perturbation in the input does not change the combinatorial solution.

An algorithm for (highly) stable instances of cut problems [BL].

18

Stable versus smooth

Consider regions induced by combinatorial solution.

In both cases, must solve all instances that are far from the boundary of their region.

For instances near the boundary:

- Smoothed analysis: solve a perturbed input.
- Stable inputs: do nothing.

19

Running example: 3SAT

$$(x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_2 \vee \bar{x}_4 \vee x_5) \wedge \cdots$$

n variables, m clauses, 3 literals per clause.

Clauses chosen independently at random.

Random formula f with m >> n.

20

Probabilistic estimates

The expected number of satisfying assignments for f is:

$$(1 - 1/2^3)^m * 2^n$$

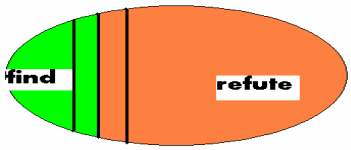
When m >> n, the formula f is unlikely to be satisfiable.

21

Two tasks

Search: if the formula is satisfiable, then find a satisfying assignment.

Refutation: if formula is not satisfiable, then find a certificate for nonsatisfiability.



2

Simple case

When m >> n log n, then if formula is satisfiable, the satisfying assignment is likely to be unique.

Then distribution on random satisfiable formulas can be approximated by planted solution distribution.

23

Planted solution model

First pick at random an assignment a to the variables.

Then choose at random clauses, discarding clauses not satisfied by a, until m clauses are reached.

When m>>n log n, a is likely to be a unique satisfying assignment.

24

Statistical properties

For every variable x, in every clause C that contained x and was discarded, the polarity of x in C disagreed with its polarity in a.

Set x according to the polarity that agrees with the majority of its occurrences in f.

When m >> n log n, it is likely that this algorithm exactly recovers a.

25

Sparser formulas

m = d*n for some large constant d.

Distribution generated by planted model no longer known to be statistically close to that of random satisfiable formulas. Favors formulas with many satisfying assignments.

We present algorithm only for planted model.

26

Majority vote

Majority vote assignment a(0).

For most variables, a(0) = a, and a(0) satisfies most clauses.

Still, linear fraction of variables disagree with a, and a linear fraction of clauses are not satisfied.

This fraction is exponentially small in d.

27

Hill climbing

Moving towards satisfying assignment.

Alon-Kahale (for 3-coloring).

Flaxman (for planted 3SAT).

Feige-Vilenchik (for semirandom 3SAT).

Semirandom model: monotone adversary can add arbitrary clauses in which all three literals are set in agreement with a.

28

Conservative local search

a(j) is the assignment at iteration j, T(j) is the set of clauses already satisfied.

a(0) is the majority vote.

Pick an arbitrary clause C not in T(j).

Find the assignment closest (in Hamming distance) to a(j) that satisfies T(j) + C.

Increment j and repeat.

29

Time complexity

The algorithm obviously finds a satisfying assignment. The only question is how fast.

The number of iterations is at most m (the number of satisfied clauses increases in every iteration).

30

Complexity per iteration

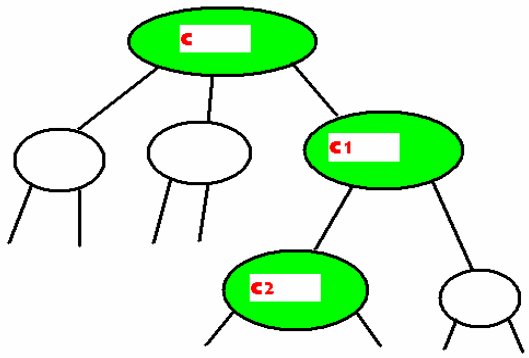
Let h be Hamming distance between a(j) and a(j+1).

At least one of three variables in C needs to be flipped.

In a clause that becomes not satisfied in T(j), at least one of two variables needs to be flipped.

Time proportional to $3 * 2^{h-1}$

31



32

Main technical lemma

Lemma: With high probability over the choice of f, in all iterations h < O(log n).

Hence algorithm runs in polynomial time.

(True also for the semirandom model.)

33

Sketch of proof – the core

A variable x for which a(0) = a is a core variable if flipping x ruins T(0), and T(0) can then be satisfied only by flipping a linear number of other variables.

The set of clauses not satisfied by the core decomposes into sub-formulas of size O(log n) not sharing non-core variables.

34

Main invariant

An iteration can be completed in O(log n) flips, of non-core variables.

As long as h = O(log n), no core variable will accidentally be flipped, and the invariant is maintained.

The algorithm need not know the core.

35

Worst case analysis

Algorithm works on every input formula f with property P (defined in terms of core).

Probabilistic analysis (much too complicated to be shown here) shows that in the planted model, input formula f is likely to have property P.

36

Open problems

Does the algorithm run in polynomial time on random satisfiable formulas?

When m >> n? For arbitrary m?

Does the cavity method (survey propagation [Braunstein, Mezard, Zecchina]) provably work on random formulas?

Alternative algorithms?

More challenging models?

37

Refutation algorithms

If the formula is not satisfiable, the algorithm presented takes exponential time to detect this.

Heuristics for finding solutions are not the same as heuristics for refutation (unlike worst case algorithms).

Common refutation algorithms (resolution) take exponential time on random formulas.

38

Refutation by approximation

When m >> n, every assignment satisfies roughly 7m/8 clauses of a random formula.

An algorithm for approximating max 3sat within a ratio strictly better than 7/8 would refute most dense 3SAT formulas.

Unfortunately, approximating max 3sat (in the worst case) beyond 7/8 is NP-hard [Hastad].

39

Turning the argument around

What if refuting random 3sat is hard?

Would imply hardness of approximation:

- Max 3sat beyond 7/8 (PCP + Fourier).
- Min bisection, dense k-subgraph, bipartite clique, 2-catalog segmentation, treewidth, etc.

A good rule of thumb. Most of its predictions (with weaker constants) can be proved assuming NP not in subexponential time [Khot].

40

A simple refutation algorithm

Assume $m > n^2$.

There are 3n clauses that contain x1.

Suffices to refute this subformula f1.

Substitute x1 = 0. Simplify to a 2CNF formula.

Random 2CNF formula with 3n/2 clauses.

Unlikely to be satisfiable.

2SAT can be refuted in polynomial time.

Repeat with x1 = 1.

41

Best current bounds

Can refute random formulas with $m > cn^{3/2}$ [Feige-Ofek].

Based on pair-wise statistical irregularities, and eigenvalue computations.

Can be run in practice on formulas with n=50000, $m = 2.5n^{3/2}$, if one trusts standard software packages for the eigenvalue computations.

42

The basic idea [Goerdt-Krivelevich]

Will be shown for random 4SAT formula f with $m > cn^2$

In a satisfying assignment a, at least half the variables are negative (w.l.o.g.).

Let S be the set of variables negative in a.

Then there is no positive clause in f whose four variables are in S.

43

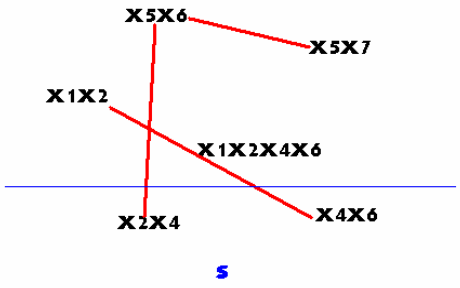
Reduction to graph problem

Every pair of variables [xi xj] – a vertex.

Every positive clause (xi xj xk xl) – an edge ([xi xj], [xk xl]).

S forms an independent set of size N/4.

44



45

Random non-satisfiable f

Random graph with N vertices and much more than N edges.

Unlikely to have an independent set of size N/4.

Moreover, this can be certified efficiently, by eigenvalue techniques (or by SDP, computing the theta function of Lovasz).

Refutes random 4SAT with $m > cn^2$

46

Extension to 3SAT

Trivially extends when $m > cn^2$

With additional ideas, get down to $m > cn^{3/2}$

A certain natural SDP cannot get below $m < cn^{3/2}$ [Feige-Ofek].

Neither can resolution [Ben-Sasson and Widgerson].

Goal: refute random 3SAT with m = O(n).

47

Summary

Several rigorous models in which to study heuristics.

Rigorous results in these models, including hardness results (not discussed in this talk).

The heuristics may be quite sophisticated.

Wide open research area.

48

Data Stream Algorithms in Computational Geometry

Timothy M. Chan
School of CS
Univ of Waterloo

INTRODUCTION

Data Stream: The Basic Model

- makes one pass over input
- uses limited (sublinear) space

Motivation

- MASSIVE data sets

Brief History [Indyk]

- Ancient times
  - (finite automata, sorting w. few passes, median [Munro, Paterson '80])
- Middle ages
- Renaissance
  - ([Alon, Matias, Szegedy '96], [Henzinger, Raghavan, Rajagopalan '98], & TONS of papers ... see Muthukrishan's survey)

Data Stream Meets CG

- diameter [Feigenbaum, Kannan, Zhang '02, Hershberger, Suri '03]
- other measure problems like width
  - [Agarwal, Har-Peled, Varadarajan '04, Chan (SoCG'04)]
- statistical problems like range counting
  - [Bagchi, Chaudhary, Eppstein, Goodrich (SoCG'04) Suri, Toth, Zhou (SoCG'04)]
- clustering problems like k-median/k-means
  - [Har-Peled, Mazumdar (STOC'04)]
- Euclidean MST/matching [Indyk (STOC'04

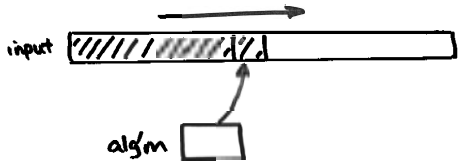
This Talk

looks at some specific examples
& some recent results

[Chan (SoCG'04),
Chan, Sadjad (ISAAC'04),
Chan, Chen [SoCG'05)]

illustrates a few techniques
& different types of
geometric streaming alg/ms

One-Pass Alg/ms



(data structures w. sublinear space
supporting inserts)

Example 0: Approx Median in 1D

Given n pts in $\mathbb{R}^1$,
find a pt of rank $\sim \frac{n}{2} \pm \varepsilon n$

Munro, Paterson's Alg/m ['80]

Standard idea: the "logarithmic" method
[Bentley, Saxe '80]

Divide set into $O(\log n)$ groups
whose sizes are distinct powers of 2

To insert:
create new group of size 1
whenever 2 groups have same size,
merge

Modified idea: "merge-and-reduce"

Replace each group with sketch

Def: R ⊆ S is a δ-sketch of S iff
i^{th} pt of R has rank $\sim \frac{in}{r} \pm \delta n$
$(n = |S|, r = |R|)$

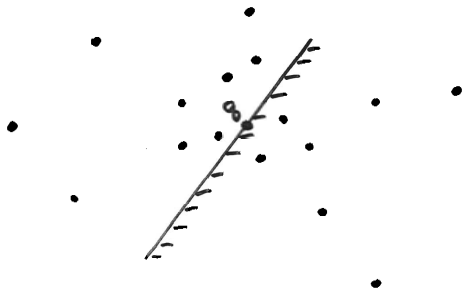
Fact: ∃ δ-sketch of size $1/\delta$

Fact: If R_j is α-sketch of S_j
$(|R_1| = |R_2|, |S_1| = |S_2|)$
then δ-sketch of $R_1 \cup R_2$ is
$(\alpha+\delta)$-sketch of $S_1 \cup S_2$

Set $\delta = \varepsilon / \log n$
$\Rightarrow$ space $O(\frac{1}{\delta} \log n) = O(\frac{1}{\varepsilon} \log^2 n)$

Example 1: Approx Centerpoint

Given n pts in $\mathbb{R}^d$,
find a pt $q \in \mathbb{R}^d$ s.t.
any halfspace containing q
contains $\geq \frac{n}{d+1} - \varepsilon n$ pts



Bagchi, Chaudhary, Eppstein, Goodrich's Algm ('04)

Idea: same method!

Def: [Vapnik, Chervonenkis '71 ... Matoušek 95]
R ⊆ S is a δ-approximation of S iff
any halfspace containing i pts of R
contains $\sim \frac{in}{r} \pm \delta n$ pts of S

Fact: ∃ δ-approximation of size
$O(\frac{1}{\delta^2} \log \frac{1}{\delta})$

$\Rightarrow$ space $O(\frac{1}{\varepsilon^{O(1)}} \text{polylog } n)$

Other Applications [BCEG'04]

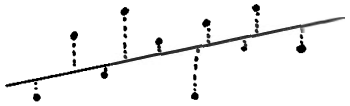
more statistics problem
(simplicial depth, LMS, ...)

range counting

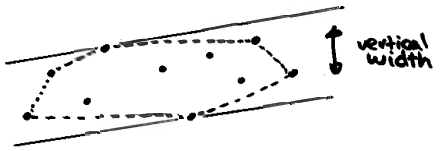
Example 2 : Approx Hyperplane Fitting

Given n pts in $\mathbb{R}^d$,

find hyperplane s.t.
max vertical distance to the pts
is minimized, to within $1+\varepsilon$ factor



i.e. minimize vertical-width of
convex hull (CH) over all directions



Agarwal, Har-Peled, Varadarajan's Alg'm [04]

Idea: logarithmic method again!

Def: RCS is a δ-core-set of S iff
$\forall$ direction x
width of CH(S) along x
$\leq (1+\delta) \cdot$ width of CH(R) along x

Fact: $\exists$ δ-core-set of size $O\left(\frac{1}{\delta^{(d-1)/2}}\right)$

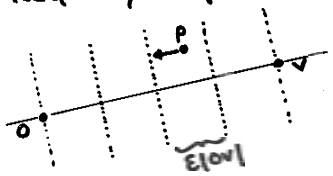
$\Rightarrow$ space $O\left(\frac{1}{\varepsilon^{O(1)}} \text{polylog} n\right)$

A New Alg'm [C'04]

Idea: "geometric-series" method

Static version: // core-sets in 2D

o = first pt
v = (approx) farthest pt from o
round pts to $\Theta(1/\varepsilon)$ grid lines
orthogonal to $\overrightarrow{ov}$
keep min/max pts on each line



Analysis: rounding error
$\leq$ · width of $\overline{ov}$ along x
$\leq$ · width of CH(S) along x

Modified streaming version:

To insert p:
whenever $|op| > 2|ov|$,
$v = p$
start a new core-set & clean up

To clean up:
keep only the b newest core-sets
round old pts to grid line thru o
keep min/max pt on line

Analysis:

rounding error $\le \frac{|pp'|}{|ov|} \cdot$ width of $\overline{ov}$ along x

$\le \frac{|op|}{|ov|} \cdot$ " " "

when p was inserted: $|op| \le 2|ov|$

at every change: $|ov|$ doubles

when p gets old: $|op| \le \frac{2|ov|}{2^b}$

$\Rightarrow$ total error $\le 2\left(\frac{1}{2^b} + \frac{1}{2^{b+1}} + \dots\right) \cdot$ width of CH(S) along x

Set $b = \log \frac{1}{\varepsilon}$

$\Rightarrow$ space $O\left(b \cdot \frac{1}{\varepsilon}\right) = O\left(\frac{1}{\varepsilon} \log \frac{1}{\varepsilon}\right)$

const (indep of n)!

Other Results & Applications [C'04]

refinement in 2D:

space $O\left(\frac{1}{\sqrt{\varepsilon}} \log^2 \frac{1}{\varepsilon}\right)$

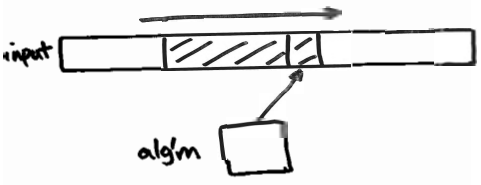
core-sets in dD:

space $O\left(\frac{1}{\varepsilon^{d-0.5}} \log^d \frac{1}{\varepsilon}\right)$

bounding box

sphere/cylinder fitting

SLIDING-WINDOW ALG/MS



(data structures supporting "insert" & "delete oldest pt")

Example: Approx Diameter in 1D

Given n pts in $\mathbb{R}^1$,

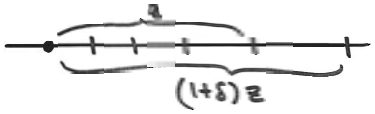
compute D = farthest distance to within $1+\varepsilon$ factor

Feigenbaum, Kanran, Zhang's Algm ['02]

Idea: logarithmic method again!

How to sketch:

forms exponentially-spaced grid
keeps newest pt (the representative) of each cell



$\Rightarrow$ space $O(\frac{1}{\varepsilon}\log\Delta\log^2 n)$

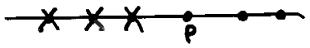
where $\Delta = \frac{\text{farthest dist}}{\text{closest dist}}$

A New (Simple!) Algm [C, Sadjad '04]

Idea: "skip-middle" method

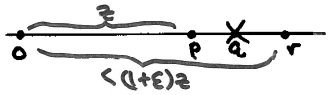
To insert p: //approx max

insert p to R
remove all pts < p from R
after $\frac{1}{\varepsilon}\log\Delta$ inserts, clean up



To clean up:

o = smallest pt of R
whenever ∃ 3 consecutive p,q,r ∈ R
s.t. $|or| < (1+\varepsilon)|op|$,
delete q from R

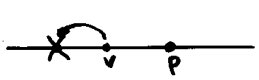


$\Rightarrow$ space $|R| = O(\frac{1}{\varepsilon}\log\Delta)$ optimal!

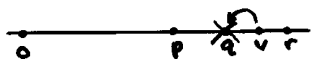
Correctness/Invariants:

1. smaller pts are newer in R
2. each pt v has a representative $v' \in R$ that is newer than v, where either
   - 2.1. v' is successor of v in R, or
   - 2.2. v' is predecessor " " " " with $|vv'| \le \varepsilon \cdot$ diameter of all pts newer than v

(insert)



(clean-up)



$(|or| \le (1+\varepsilon)|op| \Rightarrow |pv| \le \varepsilon|op|)$

Other Applications [CS'04]

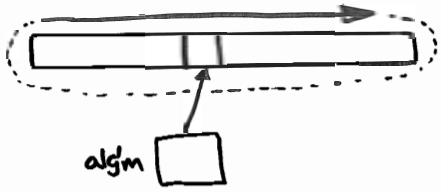
diameter in $\mathbb{R}^d$:

space $O(\frac{1}{\varepsilon^{(d-1)/2}}\log\frac{\Delta}{\varepsilon})$

[by projection]

core-sets in 2D

MULTI-PASS ALG'MS



1 Pass vs. 2 Passes, according to Knuth [AOCP, vol 1, '73]

Old lady, on a bus:

"Can you tell me how I can get off Pasadena St.?"

Boy:

"Just watch me, and get off two stops before I do."

Example 0: Exact (!) Median

Munro, Paterson's Alg'm ['80]

Idea: filtering ("prune-and-search")

$I = (-\infty, \infty)$
repeat
1. among pts inside I, compute $(1/r)$-sketch R of size $O(r)$
2. I = sub-interval containing answer

Set $r = n^\delta$

$\Rightarrow$ passes $\log_r n = \frac{1}{\delta}$ const!

space $O(r \log^2 n) = \tilde{O}(n^\delta)$ small!

Example 2 : Exact Hyperplane Fitting

$$\min t$$
$$\text{s.t. } y_i \le mx_i+b+t$$
$$y_i \ge mx_i+b-t$$
$$(i=1,\dots,n)$$

reduces to linear programming (LP) in $\mathbb{R}^{d+1}$

"New" Alg'm [C, Chen '05]

Idea: prune-&-search again

$\Delta = \mathbb{R}^d$ // LP in dD

repeat:

1. among halfspaces crossing Δ, compute $(1/r)$-cutting of size $r^{O(1)}$
2. Δ = sub-simplex containing answer

Def: Given n halfspaces, δ-cutting is a partition of space into simplices each crossed by $\le \delta n$ halfspaces

Analysis:

1. take $(1/r)$-approximation
2. solve $r^{O(1)}$ LPs in $(d-1)$D "in parallel"

passes $P_d(n) = O(P_{d-1}(n) \log_r n)$

space $S_d(n) = O(S_{d-1}(n)\, r^{O(1)} \log_r n)$

Set $r = n^{c\delta}$

$\Rightarrow$ passes $O(1/\delta^{d-1})$ const!

space $\tilde{O}(n^\delta)$ small!

Other Results [cc'05]

refinement: $O(n)$ rand time
$O(n \log\log\cdots n)$ det time in 2D

lower bd for LP in 2D:
$\frac{1}{\delta}$ passes $\Rightarrow$ $\Omega(n^\delta)$ space
[as in Munro, Paterson]

CH of sorted pts in 2D:
$O(1)$ passes, $O(n^{1/2+\delta})$ space,
$O(n)$ time

CH for small output size h in 2D:
$O(1)$ passes, $O(h n^\delta)$ space,
$O(n \log n)$ time

Conclusion

Summary of New Results

- one-pass alg'ms for ~~core-sets~~ (approx CH) [C'04]
- sliding-window alg'ms for diameter [CS'04]
- multi-pass alg'ms for LP [cc'05]

Some Open Problems

- one-pass for high dim
  - e.g. diameter: $\sim\sqrt{2}$ factor (Indyk'03]
    min enclos cylinder: ~ 5 factor [C'04]
- smallest # passes
  - e.g. LP : $d+1$ passes, $\tilde{O}(\sqrt{n})$ space [Clarkson's alg'm]
    lower bd ?

Steps into Computational Algebraic Topology

I. Topological Persistence
II. Stable Diagrams
III. Applications

I.1 Small 'n' Big Holes

I.1 Small 'n' Big Holes

I.1 Small 'n' Big Holes

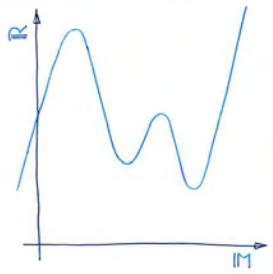
	$H_1(\mathbb{M}^\circ)$	$H_1(\mathbb{M}^{+\varepsilon})$	F_0^ε
dim	3	2	1

where $F_0^\varepsilon = \mathrm{im}\left(H_1(\mathbb{M}^\circ) \to H_1(\mathbb{M}^{+\varepsilon})\right)$.

I.2 Function

$f : \mathbb{M} \to \mathbb{R}$

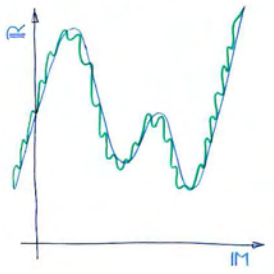
$\mathbb{M}^x = f^{-1}(-\infty, x]$



I.2 Function

$f : \mathbb{M} \to \mathbb{R}$

$\mathbb{M}^x = f^{-1}(-\infty, x]$



I.3 Persistent Homology

$\ldots \subset \mathbb{M}^x \subset \ldots \subset \mathbb{M}^y \subset \ldots$

$\ldots \to H^x \to \ldots \to H^y \to \ldots$

persistent homology groups are

$F_x^y = \mathrm{im}\,(H^x \to H^y) \subseteq H^y$

persistent Betti numbers are

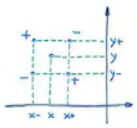
$\beta_x^y = \dim F_x^y$

I.4 Crit. Value Pairs

$\ldots \to H^{x-} \to H^{x+} \to \ldots \to H^{y-} \to H^{y+} \to \ldots$

multiplicity is

$\mu_x^y = \beta_{x-}^{y+} - \beta_{x-}^{y-} - \beta_{x+}^{y+} + \beta_{x+}^{y-}$

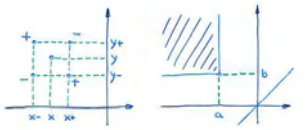


I.4 Crit. Value Pairs

$\ldots \to H^{x-} \to H^{x+} \to \ldots \to H^{y-} \to H^{y+} \to \ldots$

multiplicity is

$\mu_x^y = \beta_{x-}^{y+} - \beta_{x-}^{y-} - \beta_{x+}^{y+} + \beta_{x+}^{y-}$



$\beta_a^b = \sum_{x \le a \le b \le y} \mu_x^y$

I.2 Function

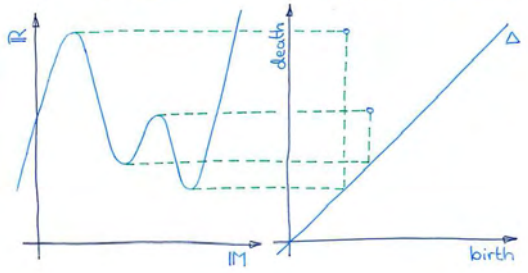
$f : \mathbb{M} \to \mathbb{R}$

$\mathbb{M}^x = f^{-1}(-\infty, x]$

II.1 Diagram

persistence diagram of f is

$D(f) = \Delta \cup \{\text{bd-pairs}\}$



I.2 Function

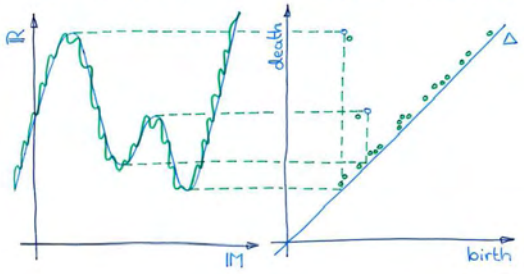
$f : \mathbb{M} \to \mathbb{R}$

$\mathbb{M}^x = f^{-1}(-\infty, x]$

II.1 Diagram

persistence diagram of f is

$D(f) = \Delta \cup \{\text{bd-pairs}\}$



II.2 Metrics

L_∞-distance between functions is

$$\|f-g\|_\infty = \sup_{x \in \mathbb{M}} |f(x)-g(x)|.$$

Fréchet bottleneck distance between diagrams is

$$d_F(D(f), D(g)) = \inf_{\gamma : D(f) \to D(g)} \sup_{p \in D(f)} \|p - \gamma(p)\|_\infty.$$

II.3 Stability Theorem

Thm [Cohen-Steiner, E, Harer 2004]

$\mathbb{M}$ is triangulable space,

$f, g : \mathbb{M} \to \mathbb{R}$ are continuous and tame.

Then

$$d_F(D(f), D(g)) \leq \|f-g\|_\infty.$$

II.3 Stability Theorem

Thm [Cohen-Steiner, E, Harer 2004]

$\mathbb{M}$ is triangulable space,

$f, g : \mathbb{M} \to \mathbb{R}$ are continuous and tame.

Then

$$d_F(D(f), D(g)) \leq \|f-g\|_\infty.$$

$\Rightarrow$ **Q Lemma** [Robins 1999]

$\varepsilon = \|f-g\|_\infty$

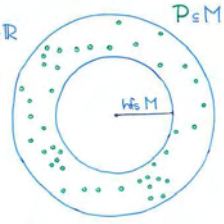
Then

$$\#(D(f) \cap Q_\varepsilon) \leq \#(D(g) \cap Q).$$

III.1 Homology Estimation

$d^M, d^P : \mathbb{R}^d \to \mathbb{R}$

distance function of M, P



hom. feature size of d^M is

$\mathrm{hfs}\, M$ = min. pos. hom. crit. value

M_x^y, P_x^y ... persistent hom. groups

III.2 Approximation

Thm. $d(P, M) < \varepsilon < \frac{\mathrm{hfs}\, M}{4}$.

Then

$$H(M) = P_\varepsilon^{3\varepsilon}.$$

Proof. $\|d^P - d^M\| < \varepsilon$.

Q Lemma implies

$$\dim M_0^{4\varepsilon} \leq \dim P_\varepsilon^{3\varepsilon} \leq \dim M_{2\varepsilon}^{2\varepsilon}$$

$$= \quad = \quad \text{because } 4\varepsilon < \mathrm{hfs}\, M$$

$$\dim(H(M)) = \dim M_0^0 = \dim M_0^{4\varepsilon}$$

□

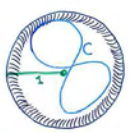
III.3 Curves

$$K(C) = \int \kappa(s)\, ds$$

$$L(C) = \frac{1}{2} \int \chi(h \cap C)\, dh$$

Fary's Thm

$L(C) \leq K(C)$.



Thm $|L_1 - L_2| \leq (K_1 + K_2 - 2\pi) \cdot d_F(C_1, C_2)$.

III.4 Surfaces

$$G(S) = \int |\kappa_1(s) \cdot \kappa_2(s)|\, ds$$

$$= 2\pi \,(\text{avg. \# crit. pts of height f.})$$

$$H(S) = \frac{1}{2} \int (\kappa_1(s) + \kappa_2(s))\, ds$$

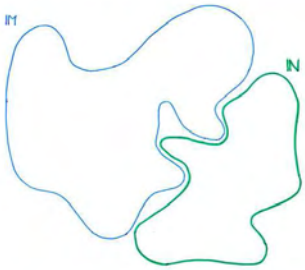
$$= \int \chi(h \cap \bar{S})\, dh$$

Thm. $|H_1 - H_2| \leq (G_1 + G_2 - 2\pi(1+g)) \cdot d_F(\bar{S}_1, \bar{S}_2)$.

II.5 Protein Interaction

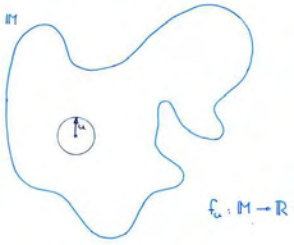
docking = comput. prediction of interacting configuration

II.5 Protein Interaction



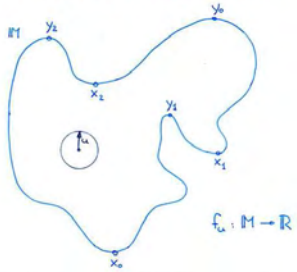
docking = comput. prediction of interacting configuration

II.6 Height 'n' Elevation



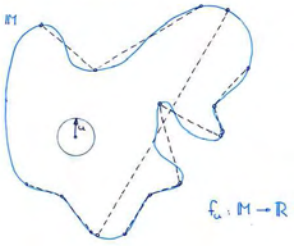
elevation is $E : M \to \mathbb{R}$ defined by
$E(x) = |f_u(x) - f_u(y)|$ with
(i) $u = \pm n_x = \pm n_y$, (ii) x, y paired.

II.6 Height 'n' Elevation



elevation is $E : M \to \mathbb{R}$ defined by
$E(x) = |f_u(x) - f_u(y)|$ with
(i) $u = \pm n_x = \pm n_y$, (ii) x, y paired.

II.6 Height 'n' Elevation



elevation is $E : M \to \mathbb{R}$ defined by
$E(x) = |f_u(x) - f_u(y)|$ with
(i) $u = \pm n_x = \pm n_y$, (ii) x, y paired.

II.7 Maxima in $\mathbb{R}^3$

four types

1- 2- 3- 4-legged

To align M with N,
fit legs in pairs to define
rigid motions.

Efficient Algorithms for the Longest Path Problem

Ryuhei UEHARA (JAIST)
Yushi UNO (Osaka Prefecture University)

The Longest Path Problem

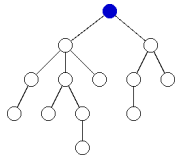
- Finding a longest (vertex disjoint) path in a given graph
- Motivation (comparing to Hamiltonian path):
  - … Approx. Algorithm, Parameterized Complexity
  - … More practical/natural
  - … More difficult(?)

The Longest Path Problem

- Known (hardness) results;
  - We cannot find a path of length n-n^{ε} in a given Hamiltonian graph in poly-time unless P=NP [Karger, Motwani, Ramkumar; 1997]
  - We can find $O(\log n)$ length path [Alon, Yuster, Zwick;1995] ($\Rightarrow O((\log n/\log\log n)^2)$ [Björklund, Husfeldt; 2003])
  - Approx. Alg. achieves $O(n/\log n)$ [AYZ95] ($\Rightarrow O(n(\log\log n/\log n)^2)$[BH03])
  - Exponential algorithm [Monien 1985]

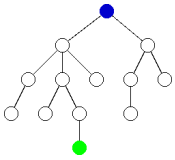
The Longest Path Problem

- Known polynomial time algorithm;
  Dijkstra's Alg.(196?): Linear alg. for finding a longest path in a tree;



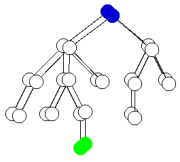
The Longest Path Problem

- Known polynomial time algorithm;
  Dijkstra's Alg.(196?): Linear alg. for finding a longest path in a tree;



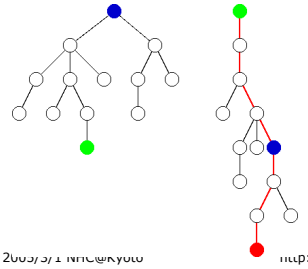
The Longest Path Problem

- Known polynomial time algorithm;
  Dijkstra's Alg.(196?): Linear alg. for finding a longest path in a tree;



The Longest Path Problem

- Known polynomial time algorithm;
  Dijkstra's Alg.(196?): Linear alg. for finding a longest path in a tree;



Approaches to the Efficient Algs to Longest Path Problem

1. Extension of the Dijkstra's algorithm
   Weighted trees (linear), block graphs (linear), cacti (O(n^2)).
   (ISAAC 2004)
2. Graph classes s.t. Hamiltonian Path can be found in poly time
   Some graph classes having interval representations (bipartite permutation, interval biconvex graphs)
   (ISAAC 2004)
3. Dynamic programming to the graph classes that have tree representations (on going)
   Cacti(linear), …

Approaches to the Efficient Algs to Longest Path Problem

1. Extension of the Dijkstra's algorithm
   Weighted trees (linear), block graphs (linear), cacti (O(n^2)).
   (ISAAC 2004)
2. Graph classes s.t. Hamiltonian Path can be found in poly time
   Some graph classes having interval representations (bipartite permutation, interval biconvex graphs)
   (ISAAC 2004)
3. Dynamic programming to the graph classes that have tree representations (on going)
   Cacti(linear), …

1. Ex of Dijkstra's Alg

Bulterman et.al. (*IPL*,2002) showed that the correctness of Dijkstra's alg stands for;

1. For each u,v,
   length of the shortest path between u and v
   = length of the longest path between u *and* v
2. For each u,v,w,
   $d(u,v) \leqq d(u,w) + d(w,v)$
3. For each u,v,w,
   $d(u,v) = d(u,w) + d(w,v)$ if and only if
   w is on the unique path between u and v

1. Ex of Dijkstra's Alg

Construct $G'=(V',E')$ from $G=(V,E)$ s.t.:

$V \subseteq V'$

For each $u,v \in V$,
length of the shortest path between u,v on G'
= length of the longest path between u,v on G

For each $u,v \in V$,
the shortest path between u,v on G' is unique

1. Ex of Dijkstra's Alg

Theorem: ExDijkstra finds a longest path if G and G' satisfy the conditions.

ExDijkstra: $G=(V,E)$ and $G'=(V',E')$

1. pick any vertex w in V;
2. find $x \in V$ with $\max\{d(w,x)\}$ on G';
3. find $y \in V$ with $\max\{d(x,y)\}$ on G';
4. x and y are the endpoints of the longest path in G, and $d(x,y)$ on G' is its length.

1. Ex of Dijkstra's Alg (Summary)

Theorem: Vertex/edge weighted tree (linear)

Theorem: Block graph (O(|*V*|+|*E*|))

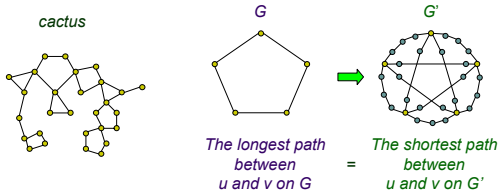
Theorem: Cactus (O(|*V*|^2))

1. Ex of Dijkstra's Alg (Cacti)

Cactus:

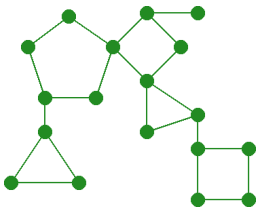
Each block is a cycle

Two cycle share at most one vertex which is a separator



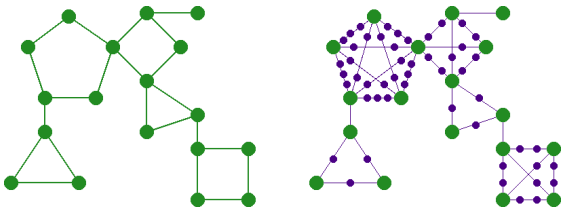
1. Ex of Dijkstra's Alg (Cacti)

Sample



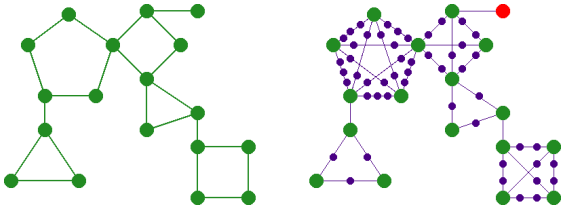
1. Ex of Dijkstra's Alg (Cacti)

Sample



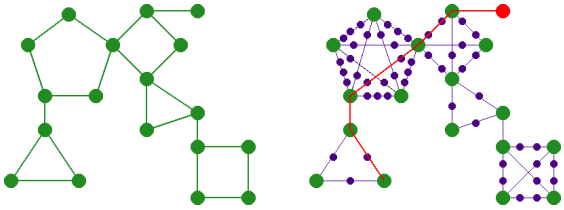
1. Ex of Dijkstra's Alg (Cacti)

Sample



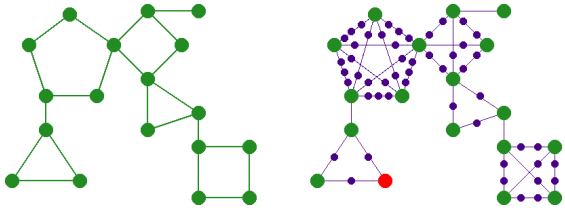
1. Ex of Dijkstra's Alg (Cacti)

Sample



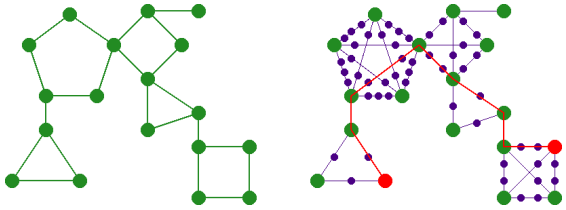
1. Ex of Dijkstra's Alg (Cacti)

Sample



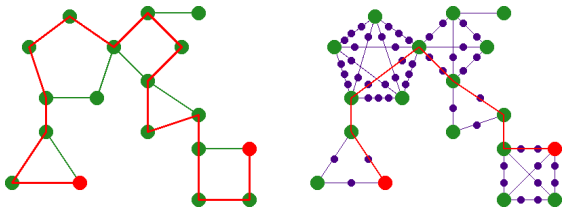
1. Ex of Dijkstra's Alg (Cacti)

Sample



1. Ex of Dijkstra's Alg (Cacti)

Sample



Graph classes s.t. Hamiltonian Path can be found in poly time

Fact 1:

Hamiltonian Path is NP-hard on a chordal graph.
(In fact, strongly chordal split graph[Müller,1997].)

Fact 2:

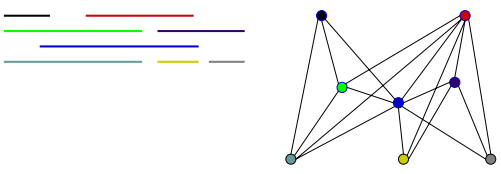
Hamiltonian Path is solvable on an interval graph in linear time. [Damaschke, 1993].

Our goal:

Poly-time algorithm for Longest Path on an interval graph.

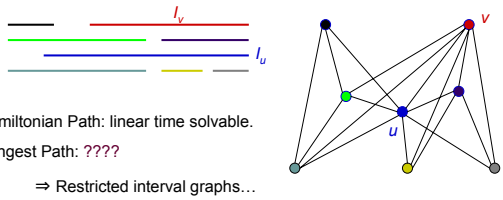
Interval Graphs

- An interval graph $G=(V,E)$ has an interval representation *s.t.* $\{u,v\} \in E$ iff $I_u \cap I_v \neq \emptyset$



Interval Graphs

- An interval graph $G=(V,E)$ has an interval representation *s.t.* $\{u,v\} \in E$ iff $I_u \cap I_v \neq \emptyset$



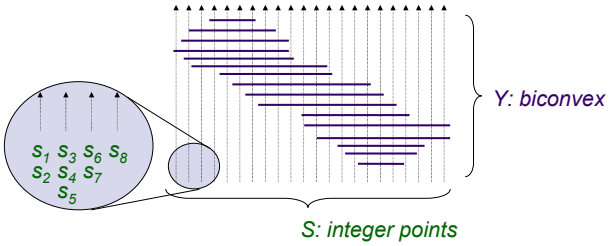
Hamiltonian Path: linear time solvable.

Longest Path: ????

⇒ Restricted interval graphs…

Restricted Interval Graphs

- An interval biconvex graph $G=(S \cup Y, E)$ has an interval representation *s.t…*

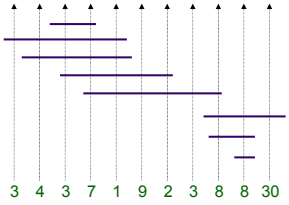


Restricted Interval Graphs

- Interval biconvex graph $G=(S \cup Y, E)$ is introduced [Uehara, Uno; 2004] from graph theoretical viewpoints;
  - ✓ *Natural analogy of biconvex graphs (bipartite graph class)*
  - ✓ *Generalization of proper interval graphs*
  - ✓ *Generalization of threshold graphs*
  - ✓ *Best possible class longest path can be found in poly time…*

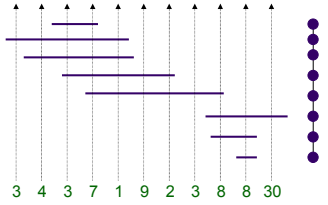
Poly-time alg for longest path on an interval biconvex graph (idea)

Find the trivial longest path P on $G[Y]$;
Embed the vertices in S into P as possible;
Adjust endpoints if necessary.



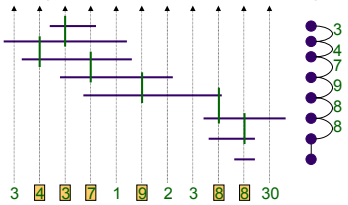
Poly-time alg for longest path on an interval biconvex graph (idea)

Find the trivial longest path P on $G[Y]$;
Embed the vertices in S into P as possible;
Adjust endpoints if necessary.



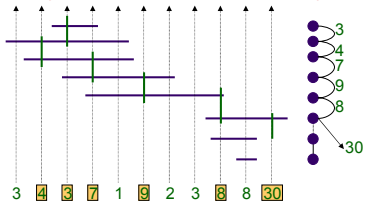
Poly-time alg for longest path on an interval biconvex graph (idea)

Find the trivial longest path P on $G[Y]$;
Embed the vertices in S into P as possible;
Adjust endpoints if necessary.



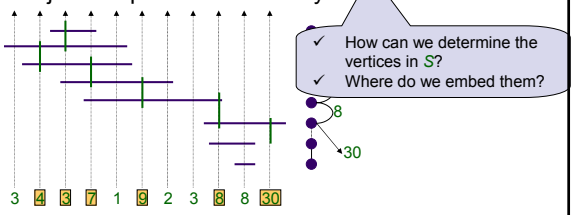
Poly-time alg for longest path on an interval biconvex graph (idea)

Find the trivial longest path P on $G[Y]$;
Embed the vertices in S into P as possible;
Adjust endpoints if necessary.



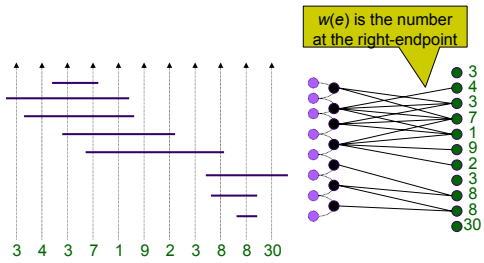
Poly-time alg for longest path on an interval biconvex graph (idea)

Find the trivial longest path P on $G[Y]$;
Embed the vertices in S into P as possible;
Adjust endpoints if necessary.



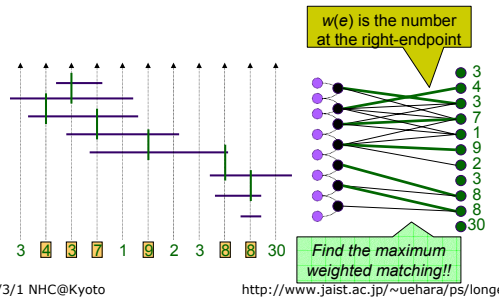
Poly-time alg for longest path on an interval biconvex graph (idea)

Embed the vertices in S into P as possible;



Poly-time alg for longest path on an interval biconvex graph (idea)

Embed the vertices in S into P as possible;



Open Problems

- Longest Path on an interval graph??
  - Combination of *DP/Dijkstra* and *weighted maximum matching* on MPQ-tree representation?
  - Related to the following open problem?
  - Hamiltonian Path *with a start point* on an interval graph? [Damaschke, 1993].
- Extension to
  - Longest cycle on some graph classes
  - Hamiltonian cycle/path on some graph classes

Proposal of Asynchronous Distributed Branch and Bound

Atsushi Sasaki†, Tadashi Araragi†,
Shigeru Masuyama‡
†NTT Communication Science Laboratories,
NTT Corporation,
Kyoto, Japan
‡Dept. of Knowledge-based Information Eng.,
Toyohashi University of Technology、
Toyohashi, Japan

Outline

- Proposal of a new framework of asynchronous branch and bound to obtain optimal solutions for discrete optimization problems where each variable denotes a host, e.g., load balancing.
- This framework is promising as it has more flexibility and robustness than conventional ones with some centralized control.

Load Balancing

- Fundamental problem to affect the performance of distributed systems
- NP-hard（e.g., Multiprocessor Scheduling [Garey, Johnson 79], Mobile Agent Allocation [Sasaki et al 05]）
- Most conventional solution methods for discrete optimization are kinds of local search [Shiragi et al, 95]
  - Further improvement from a local optimum is difficult
- Few studies focus on optimization

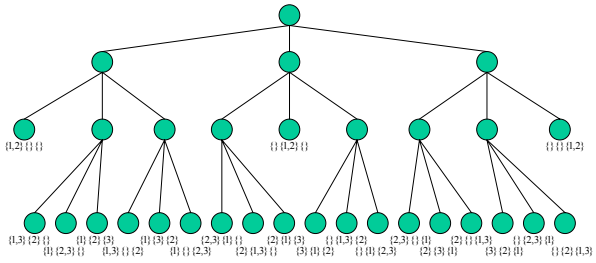
Desirable Properties

- Exact optimal solution is obtained （from any state, non-optimal solution can be improved）
- Fully distributed control
- Can be used as an approximation algorithm （especially in a large-scale system）
- Asynchronous operation
- Fault tolerance and adaptation to dynamic changes
- High performance

Conventional Branch and Bound under Distributed Environment

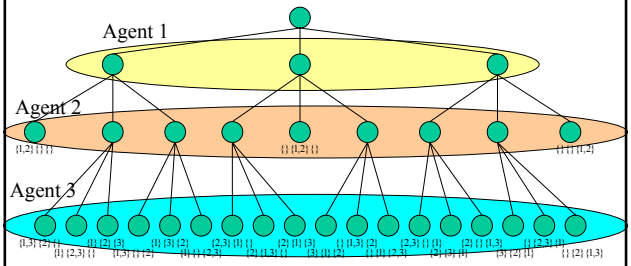
- Synchronous branch and bound [Yokoo, 01]
  - Simulating the sequential branch and bound
    - Assigning an agent to each variable and execute just like sequential branch and bound
  - Exactly one agent operates at a time (e.g., when branching is executed) so that a unique branching tree is maintained
- Distributed branch and bound[Barta et al, 02]
  - Assigning each partial problem obtained by branching operation to a different host (natural way in a distributed environment)
  - Essentially the same as the parallel branch and bound

An Example of Branching Tree in a Conventional Distributed Branch and Bound with Central Control



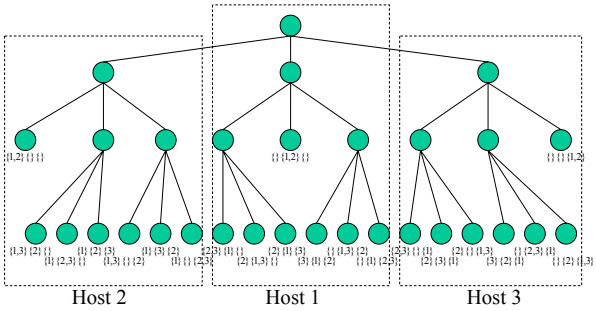
※ The case where both the number of tasks and that of hosts are 3.
※ Both of them maintain a unique branching tree.

Synchronous Distributed Branch and Bound



※ Both the number of tasks and that of hosts are 3.

Distributed Branch and Bound



※ Both the number of tasks and hosts are 3.

Drawback of the Conventional Distributed Branch and Bound

- Fragile to fault and dynamic changes
- Essentially centralized control
  - Difficult to apply to large-scale systems (as an approximation algorithm)

Strategy of Our Research

- Each host operates asynchronously and cooperate to enumerate (implicitly) all the feasible solutions
- Each host processes only information relevant to the host
- Utilize the fact that the initial state is feasible

Definition of Geographical Optimization

$$\text{Minimize} \max_i y_i(x^0, x)$$

$$\text{s.t. } x = (x_1\ x_2 \cdots x_m)^T$$

$$x_i : 1 \le x_j \le n$$

$$y_i(x^0, x) = f_i(x) + g_i(x) + k_i(x^0, x)$$

$$f_i(x) = p_i \sum_j w_j [x_j = i]$$

$$g_i(x) = \sum_{j,r} q_{x_j x_r} c_{jr} [x_j = i][x_r \neq i]$$

$$k_i(x^0, x) = \sum_j q_{x^0_j x_j} b_j [x_j = i][x^0_j \neq i]$$

$$[z] = \begin{cases} 1 & z : true \\ 0 & otherwize \end{cases}$$

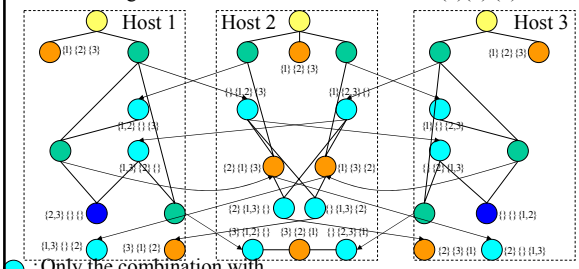
Notations for static version of Mobile Agent Allocation [Sasaki et al, 05]

x: positions of agents (described by host ID)
x^0: initial positions of agents
y: finishing time
f: CPU cost
p: CPU power of a host
w: load of an agent
g: communication cost between agents
q: communication speed of a link
c: communication amount between agents
k: migration cost of an agent
b: size of an agent at migration]

Asynchronous Distributed Branch and Bound (Asynchronous DBB)

(n=3, m=3) Host 1 Host 2 Host 3

Undirected edges denote those of the network, and (1)(2) (3): initial state



: Only the combination with initial state is deleted.

: terminated as its lower bound >y_0 ({1}{2}{3})

: a state with migration to an adjacent host

: feasible solution left (when y_0 unchanged)

Basic Operations of the Proposed Asynchronous Distributed Branch and Bound(Asynchronous DBB)

- Update of the incumbent value:
  - New value is spread in the system by flooding
- Branching Operation:
  - Generate a new state by combining at least two states
  - Notify adjacent hosts of the state with migration
  - Compute cooperatively the objective function of each state
- Bounding Operation:
  - Terminate a state from which no optimal solution is derived
  - Notify adjacent hosts of the terminated state, if necessary

※ State: combination of variable values that is a candidate of a solution where migration is also considered

Messages used in the Asynchronous DBB

- Update of the incumbent value: *update*(*y'*,*a'*)
- Branch operation:
  - Branch: *migrate*(x_j,*s*), *local_improve*(*s*,*y'*)
  - Computation of objective function: *local_max*(*s*,*y'*,*a'*), *local_max_fix*(*s*,*y'*,*a'*)
- Bound operation: *bound*(*s*,*a'*)

s:state (represented by the difference from the initial state), *y'*: objective function value of *s*, *a'*: host from which the message was sent (source host of the message)

Outline of the Operation at initial state

- Incumbent value ← the current value of the objective function
- Generate a state where variables are migrated to adjacent hosts from the current hosts
- Notify adjacent hosts of the state *s* and variable x_j to be migrated using message *migrate*(x_j,*s*)

Other operations are triggered by some message

An Example of Operations at the Initial State

- The case where h_1 (adjacent host: h_2) has only variable x_1:
  - Initialization of the incumbent value :$y=y_0$, $a=a_0$
  - Generate a state where variable x_1 is to be migrated to h_2, then send $migrate(x_1, x^0)$ to h_2
- The generated state is put into *I*

Set *S*: set of enumerated states at present:
S has only x^0 at the initial state.

Set *S'*: a terminated state whose descendants may yield a better value than the incumbent value: Φ at the initial state

Operation when *Update* is Received

- If the value *v* carried by the message is smaller than the incumbent value *z*, update the incumbent value to *v* and send it to hosts other than the source of the message.
  - If there is a state terminated by the update of the incumbent value, then bounding operation is executed.
- If $v > z$, then do nothing.
  - If $v = z$, then tie breaking is done according to ID of each host.

Operation when *bound* is Received

- If the *bound* has been received previously, ignore it.
- Remove the state attached to the message from *S*
  - If further branching may yield a good solution, then append the state to *S'*
  - If migration of a variable from some other host becomes impossible by the removal of the state, then send *bound* to the host.
- If the attached state does not have migration, then send it to hosts excluding the source of the message.

Operation when *Migrate* is received

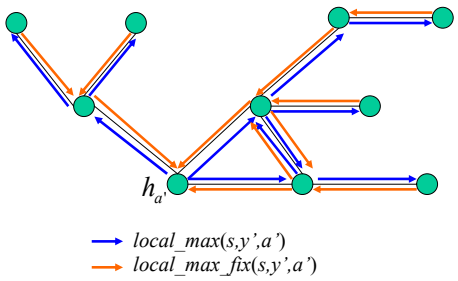
- Generate a state where variables to be migrated are set in it and combine the state and states in *S*, S' to generate a new state. (enumeration)
- Assign its objective function value to *v* of the generated state. If $v>z$ where *z* is the incumbent value, then terminate the state.
- If the non-terminated generated state has migration, then notify the destination of the migration by sending *migration*.
- If all the variables in the non-terminated generated state is fixed, then send *local_max* to compute its objective function value.

Computation of the Objective Function Value

- *local_max*(*s*,*y'*,*a'*)
  - Spread the object function value *y* of state *s* at host $h_{a'}$
- *local_max_fix*(*s*,*y'*,*a'*)
  - Used for fixing the objective function value spread by the above operation.
  - The objective function value is fixed to *y'* when host $h_{a'}$ receives this message from all the adjacent hosts.
- Computation is done only at hosts that is changed from the initial state.
  - If this is not the case of h_{a_0}, then *local_improve* is sent to h_{a_0}
- Multicast, instead, can be applicable.

※:h_{a_0} host that gives the objective function value at the initial state.

How to Obtain the Value of the Objective Function



Termination

- Terminate when no message is in the distributed system

⇒ incumbent values at different hosts are the same

- A state which gives the incumbent value exists in *S* at some host ⇒ the incumbent value is the optimal solution

※ *S*: set of states currently enumerated

Correctness

- The incumbent value is integer and monotonically decreasing⇒it reaches to the optimal value if enumeration is realized
- Enumeration (excluding terminated states) : realized by message *migrate* and message *local_improve*

Discussion on Properties and Future Prospects

- Approximation
- Combining some other approximation methods
- Coping with large-scale systems
- Asynchronous operation
- Fault tolerance and flexibility for the dynamic change
- Efficiency

Approximation

- The solution corresponding to the incumbent value provide an approximation solution as is the case of sequential branch and bound
- If migration costs are high, optimal solution may be obtained earlier.

Using Some Other Approximation Method to Obtain an Upper Bound

- Introducing an upper bound computed by some approximation algorithm may helpful for cutting the branching tree
- Thus, developing an efficient distributed approximation algorithm may help

Coping with Large-scale Systems

- Seamless decomposition is realized by restricting the length of movement for each variable.
- By this restriction, the number of messages may be reduced drastically from $O(m)$
- However, the incumbent value should be carefully treated.

Asynchronous Operation

- Proposed asynchronous DBB is highly asynchronous as operations at each host are triggered by messages and relation among processing of different hosts are not strong.
- This property may help improve the efficiency, e.g., by assigning priority of processing for each message
  → This is one of the important topics for future research

Fault Tolerance and Coping with dynamic change

- Asynchronous DBB can partialy cope with them.
  - Failure at a host where the objective function at initial state is not maximal and different from the current incumbent value can be torelated
  - Appending a new host
  - Appending a new variable(only when the value of the objective function does not exceed the incumbent value).
- Other cases are left for future research
  - Including the modeling issues, e.g., how to treat variables on the failure host

Efficiency

- Searching strategy used in sequential branch and bound cannot be straightforwardly applied to asynchronous DBB → searching strategies fit for asynchronous DBB should be developed.
- The number of messages and that of memories required is very large
  - Some reduction method of messages and memories is required

Conclusion

- A new framework of asynchronous distributed branch and bound (asynchronous DBB) was proposed.
- Asynchronous DBB is promising from the viewpoint of fault tolerance and flexibility
- This may become an infrastructure for future large-scale distributed system

Future Research Topics

- Considering fault tolerance and adaptaion to dynamic changes（including modeling）
- Considering how to improve efficiency
  - Examination of detailed operations（e.g., whether a message can be sent or not）
    （e.g., message reduction）
  - Considering branching order
  - Reduction of space complexity
- Considering good distributed approximation algorithm for obtaining upper bound
- Experiments for evaluation
- Coping with mixed integer programming

Energy-Optimal Online Algorithms for Broadcasting in Wireless Network

Shay Kutten
Hirotaka ono
David Peleg
Kunihiko Sadakane
Masafumi Yamashita

Outline

- Background
- Model
- Problems and Results
- Algorithms and Analyses
  - Single Receiver Case
  - Multiple Receivers Case
- Conclusion

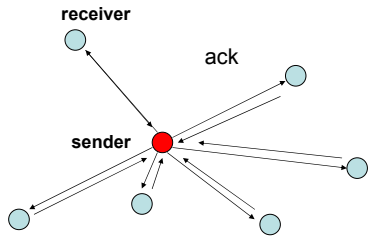
Background

- Design energy-efficient online message broadcasting protocols in ad-hoc wireless networks

  – energy-efficiency :
    - save the battery-resource

  – online property: ··· ad-hoc network
    - non-static network

Problem



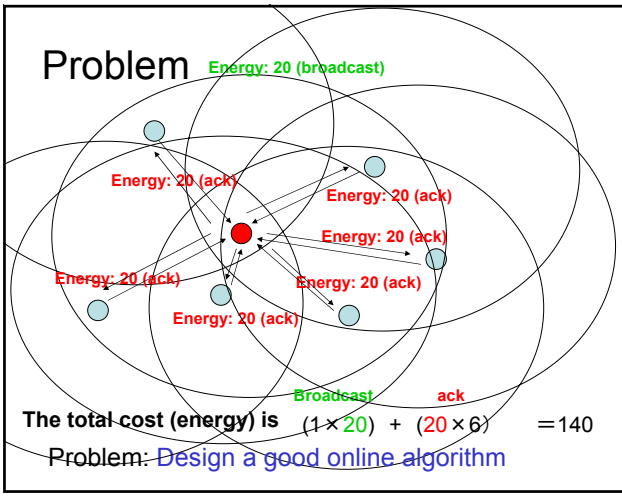
- The sender does not know the distances to receivers
- Broadcast a message to nearest *n-1* hosts
- Receiving ack from the *n-1* hosts

Problem: Design a good online algorithm

Problem

- Communication requires energy consumption.
- The energy consumption depends on the distance between the sender and receivers. (The distance is longer, the energy must be larger.)
- The **s**ender/**r**eceiver have no distance information.
- **s** sends some message (e.g., beacon) to **r.** with some energy consumption.
- If **r** receives the beacon, he needs to send “ack” to **s** with the same amount of energy consumption.

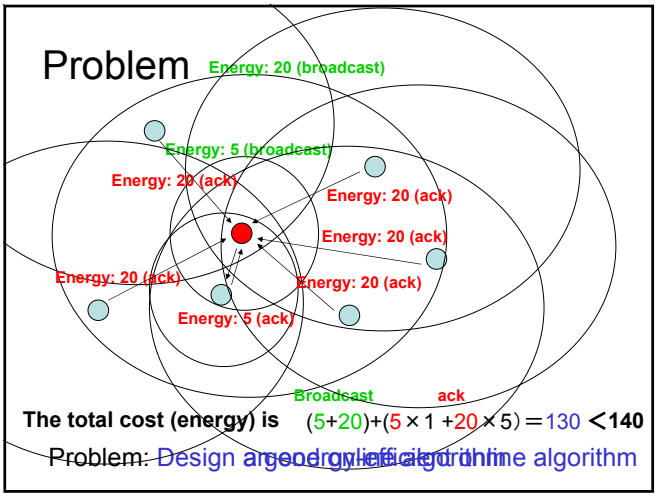
Problem



The total cost (energy) is $(1 \times 20) + (20 \times 6) = 140$

Problem: Design a good online algorithm

Problem



The total cost (energy) is $(5+20)+(5\times 1+20\times 5)=130 < 140$

Problem: Design an energy-efficient online algorithm

Model

- The attenuation of signal power P_s is $\tilde{P}_s = \frac{P_s}{d(s,t)^\delta}$ where $d(s,r)$ is the distance between s and r, and $\delta \geqq 1$ is the distance-power gradient.
  γ is the minimum power to decode a message.
  - The maximum distance to which a message can derived from s is $(P_s/\gamma)^{1/\delta}$
- Only a direct broadcast is allowed. (No multi-hop delivery is allowed.)
- Synchronous Communication ⋯ (We can utilize a global clock and unique IDs of nodes)
- Collision-free and Failure-free

Related Works

- Range Assignment Problem
  - offline : The distances between any pair of hosts are given.
  - Minimizing the total energy consumption to broadcast a message to a set of recipients
  - Constructing energy-efficient multicast tree with several properties:
    - connectivity from a source, strong connectivity, small radius, and so on

"On the Complexity of Computing Minimum Energy Consumption Broadcast Subgraphs", [CCPRV 2001]

"Power Consumption in Packet Radio Networks", [KKKP 2000]

Problems and Results

Algorithms and its Performance

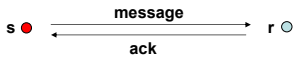
- Minimize the total energy consumption
- Our model is "online", i.e., no a-priori information.
- Use competitive analysis:
- The performance of algorithm A (competitive ratio) is

$$\sup\left\{\frac{\text{cost}(A,I)}{\text{cost}^*(I)}\middle| I : \text{instance}\right\}$$

- cost* : the minimum value of the total energy consumption with complete information

Problems and Results (1)

- **Problem BA2** (Broadcast+Ack-2)
  - one sender *s* and one receiver *r*
  - s sends a message to *r*.
  - *r* sends an ack to s after receiving the message.



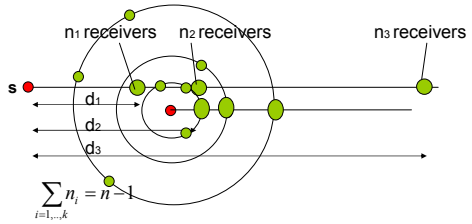
  - $\text{cost}^* = 2p^* = 2\gamma \cdot d^\delta$
- **Theorem**

  The optimal competitive ratio of problem BA2 is $3/2+\sqrt{2}$

  (No online algorithm whose competitive ratio is smaller than $3/2+\sqrt{2}$ **)**

Problems and Results (2)

- **Problem BAn** (Broadcast+Ack-n)
  - one sender *s* and n-1 receivers, $r_1, r_2, \ldots, r_{n-1}$
  - s sends a message to $r_1, r_2, \ldots, r_{n-1}$.
  - Each r sends an ack to s after receiving the message.



Problems and Results (3)

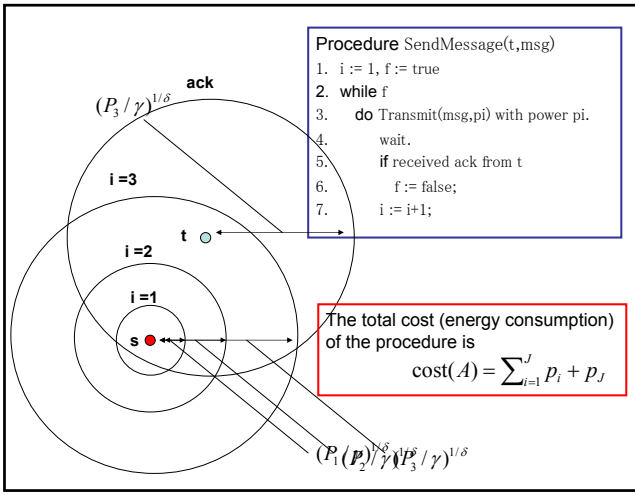
Theorem

The optimal competitive ratio of problem BAn is $3/2+\sqrt{2}$.

Algorithms and Analyses

Generic Protocol (Algorithm)

```
Procedure SendMessage(t,msg)
1. i := 1, f := true
2. while f
3.    do Transmit(msg,pi) with power pi.
4.       wait.
5.       if received ack from t
6.          f := false;
7.       i := i+1;
```




```
Procedure SendMessage(t,msg)
1.  i := 1, f := true
2.  while f
3.     do Transmit(msg,pi) with power pi.
4.        wait.
5.        if received ack from t
6.           f := false;
7.        i := i+1;
```

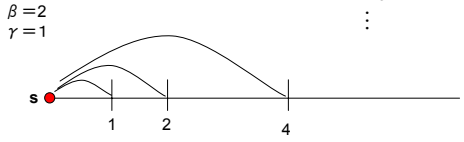
The total cost (energy consumption) of the procedure is

$$\text{cost}(A) = \sum_{i=1}^{J} p_i + p_J$$

Single Receiver Case (1)

- **Algorithm: DA[β]** (Doubling Algorithm)
  - In SendMessage,
    Set $p_1 = \gamma$ and $p_{i+1} = \beta \cdot p_i$.

$$p_1 = \gamma$$
$$p_2 = \gamma \cdot \beta$$
$$p_3 = \gamma \cdot \beta^2$$
$$\vdots$$



Single Receiver Case (2)

- **Proposition**:
  DA[β] algorithm achieves the competitive ratio is $\frac{\beta(2\beta-1)}{\beta-1}$ for problem BA2.

The value $\frac{\beta(2\beta-1)}{\beta-1}$ is minimized when $\beta = 1+\frac{1}{\sqrt{2}}$,

and it is $\frac{3}{2}+\sqrt{2}$.

Single Receiver Case (3)

- Theorem
  The optimal competitive ratio of problem BA2 is $3/2+\sqrt{2}$

Sketch of Proof:

1. Assume an optimal online algorithm with competitive ratio c ≦ 3/2+√2 and its output, say x_1, x_2, x_3 ….
2. From the competitive ratio property, we have the following inequality,
$$x_{i+1} \le \alpha_i \cdot x_i,\ \alpha_i = c+\frac{1}{2}-\frac{c}{\alpha_{i-1}}$$

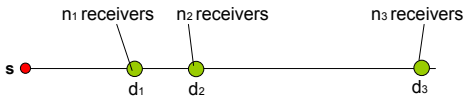
Sketch of Proof: (continued)

3. The parameter sequences α_i is a Cauchy sequence, so α_i converges to a real value α, and we have the following quadratic equation:
$$\alpha = c+\frac{1}{2}-\frac{c}{\alpha}$$
4. From the condition of the existence of α is
$$c \ge \frac{3}{2}+\sqrt{2}$$
5. The algorithm achieves the competitive ratio; i.e., it gives the upper bound.

Q.E.D

Multiple Receivers Case(0)

- **Problem BAn** (Broadcast+Ack-n)
  - one sender *s* and n-1 receivers, $r_1, r_2, \ldots, r_{n-1}$
  - s sends a message to $r_1, r_2, \ldots, r_{n-1}$.
  - Each r sends an ack to s after receiving the message.

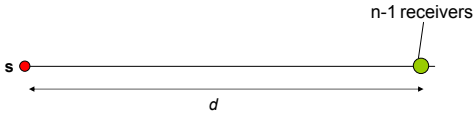


- Offline case:
  A simple Dynamic Programming can solve this in liner time.

Multiple Receivers Case (1)

Consider a simple special case:

- **Problem UBAn** (Broadcast+Ack-n)
  - one sender *s* and n-1 receivers, $r_1, r_2, \ldots, r_{n-1}$ all at the same distance d from s.
  - s sends a message to $r_1, r_2, \ldots, r_{n-1}$.
  - Each r sends an ack to s after receiving the message.



Multiple Receivers Case (2)

- **Proposition**
  The competitive ratio of DA[β] algorithm fixing $\beta = 1+\frac{1}{\sqrt{n}}$, for UBAn is at most $1+\frac{2}{\sqrt{n}}+\frac{1}{n}$

- **Theorem**
  The optimal competitive ratio of problem UBAn is $1+\frac{2}{\sqrt{n}}+\frac{1}{n}$

The previous proofs can be extended to this case.

Dynamic Doubling Algorithm

To solve the general case, we propose the following online algorithm:

```
Procedure DDA(n,msg)
1. p:= γ
2. while n>1
3.    do Transmit(msg,p) with power p.
4.       wait.
5.          n:=n−#(received ack)
6.          p:= p・β_n
```

$\beta_k = 1 + \frac{1}{\sqrt{k}}$

Results of Multiple Receivers (1)

Theorem

The optimal competitive ratio of problem BAn is $3/2+\sqrt{2}$.

Sketch of Proof:

- Lower bound : Consider the following situation (instance):

This dominates the total energy consumption.

Sketch of Proof:

- Upper bound : DDA algorithm achieves the competitive ratio $3/2+\sqrt{2}$.

1. The problem instance can be considered the union of $UBAn_1$ and $BA(n-n_1)$.
2. In the $UBAn_1$ part, DDA algorithm achieves competitive ratio $1+\frac{2}{\sqrt{n_1}}+\frac{1}{n_1} \le \frac{3}{2}+\sqrt{2}$
3. By applying this discussion repeatedly, the competitive ratio of each part is at most $3/2+\sqrt{2}$, so in total the competitive ratio is $3/2+\sqrt{2}$.

Q.E.D

Conclusion

- Direct broadcast on online setting
- Single receiver and multiple receivers
- Energy-optimal online algorithms
  - doubling algorithm and dynamic doubling algorithm
  - The optimal competitive ratios are both $3/2+\sqrt{2}$

Future Work

- Not only energy-efficient but also time-efficient online algorithm
- Considering failure, collision, and so on

Ultimate Implementation and Analysis of the AMO Algorithm for Approximate Pricing of European-Asian Options

Akiyoshi Shioura
(Tohoku University)

joint work with T. Tokuyama

Summary of This Talk

- option: typical financial derivative
- pricing European-Asian option on binomial model
  --- difficult to compute accurately
  ⇒ approximation
- Aingworth, Motwani & Oldham (SODA00)
  time: $O(kn^2)$, absolute error $O(nX/k)$
- Our Algorithm:
  time: $O(kn^2)$, absolute error $O(X/k)$

n, X: problem parameters, k: time-error trade-off param.

Option

- option: right to sell (or buy)
  some financial asset (e.g., stock)
  at some point in the future (expiration date)
  for a specified price (strike price)
- gain more benefit by investment
- hedge risk from the fluctuation of stock price

Payoff of Option

Example: option to buy a stock of Google Inc.
at the year-end at $200

stock price goes up to $220 at the year-end
⇒ exercise option to buy the stock at $200
⇒ sell it for $220 ⇒ gain $20 (payoff)

stock price goes down to $170
⇒ do not exercise option ⇒ payoff = $0

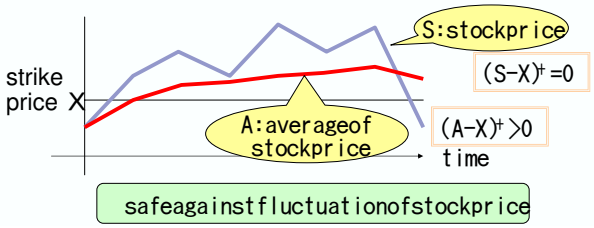
Google

Payoff of European Option:
$(S - X)^+ = \max\{S - X, 0\}$
(S: stock price at expiration date, X: strike price)

European-Asian Option

- payoff of European-Asian option
  depends on average of stock price A
  during whole period

payoff: $(A - X)^+ = \max\{A - X, 0\}$

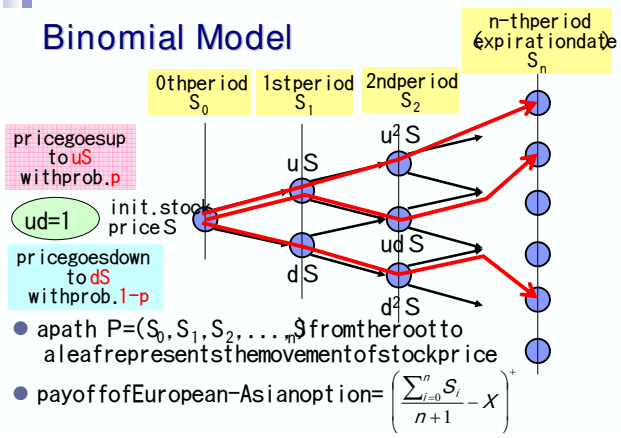


safe against fluctuation of stock price

Computation of Option Price

- price of option = discounted expected value of payoff
  --- need to model the movement of stock price
- Our model: binomial model (discrete model)
  - proposed by Cox, Ross & Rubinstein (1979)
  - represent stock price movement
    by a binomial tree
  - can compute exact option price by DP

Binomial Model



- a path $P=(S_0, S_1, S_2, \ldots, S_n)$ from the root to a leaf represents the movement of stock price
- payoff of European-Asian option = $\left(\frac{\sum_{i=0}^{n} S_i}{n+1} - X\right)^+$

Our Problem

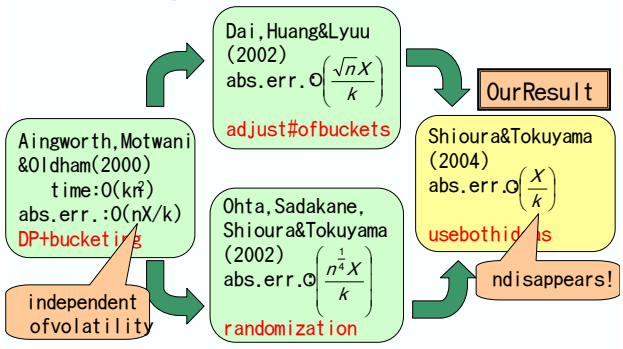
compute the expected payoff of European-Asian option on the binomial model $E\left[\left(\frac{\sum_{i=0}^{n} S_i}{n+1} - X\right)^+\right]$

- payoff is dependent on the path $P=(S_0, S_1, S_2, \ldots, S_n)$ (path-dependent option)
- payoff is nonlinear w.r.t. the running total $\sum_i S_i$
  ⇒ need enumeration of all the paths
  ⇒ exponential time
- computation of the price of path-dependent option is #P-hard

Approximation Algorithms for Pricing European-Asian Option

- Monte Carlo Method
  - based on path sampling
  - error bound depends on the volatility of stock price
- Other methods
  - based on heuristics
  - no theoretical error bound

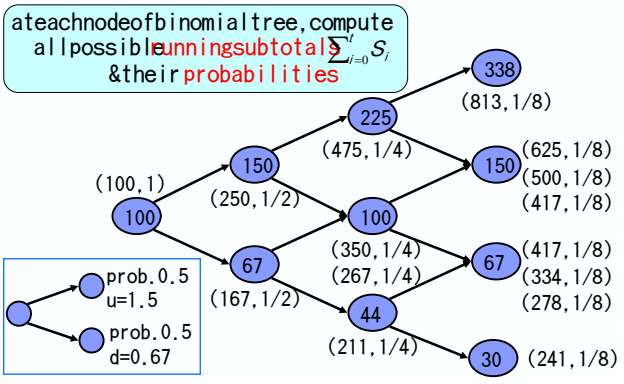
AMO Algorithm and its Variants



(n: depth of binomial tree, X: strike price, k: positive integer)

Exact Algorithm by DP

at each node of binomial tree, compute all possible running subtotals $\sum_{i=0}^{t} S_i$ & their probabilities



AMO Algorithm (1)

- # of running subtotals can be exponential
  ⇒ approximate running subtotals by bucketing

interval	running subtotal & probability
400 300	(310, 0.05)
300 200	(205, 0.15) (240, 0.12) (285, 0.20)
200 100	(170, 0.10) (150, 0.10) (110, 0.10)
100 0	(80, 0.05) (30, 0.01)

roundup running subtotals & sumup probabilities in each bucket

400 300	(400, 0.05)
300 200	(300, 0.47)
200 100	(200, 0.30)
100 0	(100, 0.06)

AMO Algorithm (2)

- k:#ofbucketsateachnode
  ⇒ errorbound ≦ max.valueofrunningsubtotal/k

Proposition:
runningsubtotal $\sum_{i=0}^{t} S_i$ ≧ (n+1)X atthet-thperiod

optionwillbeexercisedattheexpirationdate
conditionalexpectationofthepayoff
canbecomputedeasily

⇒ errorboundofAMOalgorithm= (n+1)X/k

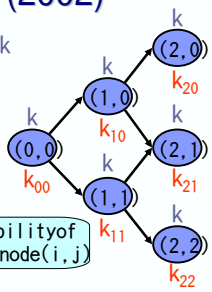
Algorithm by Dai et al. (2002)

AMOalgorithm :usethesamenumber k ofbucketsateachnode

setthe numberofbucketsk $_{ij}$ atthenode(i,j)flexibly

errorbound $\sum_{i=0}^{n}\sum_{j=0}^{i}\frac{X}{k_{ij}}\omega(i,j)$

probabilityof reachingnode(i,j)



- adjust#ofbucketsk $_{ij}$ tominimizeerrorbound underthecondition $k_{ij}=kn^2$

errorbound $O\left(\frac{\sqrt{n}X}{k}\right)$

Algorithm by Ohta et al. (2002)

AMOalgorithm :approximaterunningsubtotals inabucketby rounding-up

choosearunningsubtotal randomly asapproximatevalue

interval	running subtotal & probability
200	(170, 0.30)
	(150, 0.10)
100	(110, 0.20)

prob.1/2 → (200,0.60) (170,0.60)
prob.1/6 → (150,0.60)
prob.1/3 → (110,0.60)

Analysis of Ohta et al. (2002)

- regardthebehaviorofrandomizedalgorithm as stochasticprocess⇒ Martingale
  expectationoftheerrorbyrandomchoice ofrunningtotalsatanode=0

⇒ applyAzuma'sinequality(1967)

error bound $O\left(\frac{n^{\frac{1}{4}}X}{k}\right)$ (with high probability)

analysisisdifficult

Our Algorithm

- setthe numberofbucketsk $_{ij}$ atnode(i,j)flexibly
- randomchoiceofrunningsubtotal

errorbound $O\left(X\sqrt{\sum_{i=1}^{n}\sum_{j=0}^{i}\left[\frac{\omega(i,j)}{k_{ij}}\right]^2}\right)$

- adjust#ofbucketsk $_{ij}$ tominimizeerrorbound underthecondition $k_{ij}=kn^2$

errorbound $O\left(\frac{X}{k}\right)$

analysisisquiteeasy!

Open Problems

- derandomization of our algorithm with the same error bound
- approximation of American-Asian option
- analysis of error bound compared to exact price

On Computing all Abductive Explanations from a Propositional Horn Theory

Kaz Makino
(Graduate School of Engineering Science, Osaka Univ.)

Joint work with Thomas Eiter
(Technische Universität Wien)

Outline

1. 3 reasoning mechanisms
2. Abduction from Horn theories
3. Generating abductive explanations from Horn theories
4. Model-based representation for Horn theories

3 Reasoning Mechanisms

Deduction: fact $\cup$ knowledge base $\models$?

Induction: fact $\cup$? $\models$ observation

Abduction: ? $\cup$ knowledge base $\models$ observation

Deduction

- Fact: battery is down
- knowledge: if the battery is down, the car will not start

……

⇨ The car will not start

3 Reasoning Mechanisms

Deduction: fact $\cup$ knowledge base $\models$?

Induction: fact $\cup$? $\models$ observation

Abduction: ? $\cup$ knowledge base $\models$ observation

Induction

- Fact: battery is down
- Observation: The car will not start

⇨ Rule: if the battery is down, the car will not start

3 Reasoning Mechanisms

Deduction: fact $\cup$ knowledge base $\models$?

Induction: fact $\cup$? $\models$ observation

Abduction: ? $\cup$ knowledge base $\models$ observation

Abduction

- knowledge: if the battery is down, the car will not start

……

- Observation: The car will not start

⇨ Fact: battery is down

Abduction (formulated by C.S. Peirce ' 31-' 58)

Widely used in Computer Science and AI

Basis for

Truth Maintenance Systems (TMS, ATMS)
Clause management Systems (CMS)
Diagnosis
Database Update, ...

Propositional Horn Knowledge Base

Propositional variables: $x_1, x_2, \cdots, x_n \in \{0,1\}$

Knowledge $f : \{0,1\}^n \to \{0,1\}$

CNF (conjunctive normal form): E.g.,

$$\varphi = (\overline{x}_2 \vee \overline{x}_3 \vee x_4)(\overline{x}_3 \vee \overline{x}_4 \vee x_2)(\overline{x}_2 \vee x_1)$$

Horn CNF: at most 1 positive literal in each clause

Propositional Horn Knowledge Base

Horn CNF: at most 1 positive literal in each clause

$$\varphi = (\overline{x}_2 \vee \overline{x}_3 \vee x_4)(\overline{x}_3 \vee \overline{x}_4 \vee x_2)(\overline{x}_2 \vee x_1)$$

Horn clause: $(\overline{x}_{i_1} \vee \overline{x}_{i_2} \vee \cdots \vee \overline{x}_{i_k} \vee x_{i_0})$

Horn rule: $x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_k} \to x_{i_0}$

(antecedent/consequent: may be empty)

$$\varphi^* = (x_2 x_3 \to x_4)(x_3 x_4 \to x_2)(x_2 \to x_1)$$

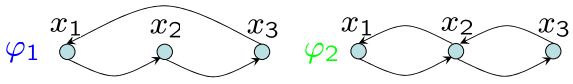
Core language in AI and logic programming

Horn CNF representation is not unique

E.g.,

$\varphi_1 = (x_1 \to x_2)(x_2 \to x_3)(x_3 \to x_1)$

$\varphi_2 = (x_1 \to x_2)(x_2 \to x_1)(x_2 \to x_3)(x_3 \to x_2)$



$$mod(\varphi_1) = mod(\varphi_2) = \{(111), (000)\}$$

$$\| $$

$$\{v \in \{0,1\}^n \mid \varphi_1(v) = 1\}$$

Explanations

φ: a Horn CNF

q : a propositional variable

An explanation for q from φ: a minimal set E s.t.

(1) $\varphi \cup E \models q$

(2) $\varphi \cup E$ is satisfiable

$\varphi \cup E \equiv \varphi \wedge \bigwedge_{x \in E} x$

$\varphi \models \psi$: $\varphi(v) = 1$ implies $\psi(v) = 1$ for all $v \in \{0,1\}^n$

(1) $\varphi \models (\bigwedge_{x \in E} x \to q)$

(2) $\exists v \in mod(\varphi)$ s.t. $(\bigwedge_{x \in E} x)(v) = 1$

Explanations

φ: a Horn CNF

q : a propositional variable

An explanation for q from φ: a minimal set E s.t.

(1) $\varphi \cup E \models q$

(2) $\varphi \cup E$ is satisfiable

Abduction: $\underset{E}{?} \cup$ knowledge base $\models$ observation

φ $\quad$ q

E.g., Explanations for x_1 from

$$\varphi = (x_2 x_3 \to x_4)(x_3 x_4 \to x_2)(x_2 x_3 \to x_1)$$

$\varphi \cup \{x_1\} \models x_1$

$\varphi \cup \{x_2, x_3\} \models x_1$

$\varphi \cup \{x_3, x_4\} \models x_1$

(1) $\varphi \cup E \models x_1$

(2) $\varphi \cup E$ is satisfiable

$$E = \{x_1\}, \{x_2, x_3\}, \{x_3, x_4\}$$

$E = \{x_1\}$: trivial explanation for x_1

Well-known:

Finding a nontrivial explanation E is poly. time.

Finding an explanation $E \subseteq A$ is NP-hard.

(Selman & Levesque '90)

Abduction: $\underset{E}{?} \cup$ knowledge base $\underset{\varphi}{\models}$ observation $\underset{q}{}$

Car diagnosis

φ: if the battery is down, the car will not start
if the gas tank is empty, the car will not start
.....
q: The car will not start

⇨ E: {battery is down}, {gas tank is empty}, …

1. Generate all possible explanations
2. Find a real one from them

Can we generate all (poly. many) explanations efficiently ?

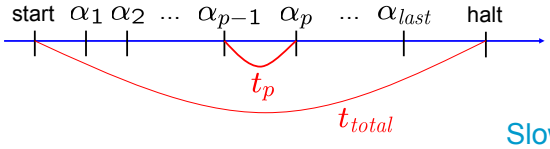
Conjecture by Selman & Levesque ('90)
Generating $O(n)$ explanations is NP-hard, even if there are only few explanations overall.

Eiter & Makino (2002) disproved it

Note: Exponentially many explanations might exist.

$\varphi = \bigwedge_{i=1}^{n} (x_i \to y_i) \wedge (y_1 y_2 \ldots y_n \to q)$
$\mathcal{E} = \{\{e_1, e_2, \ldots, e_n\} \mid e_i \in \{x_i, y_i\}\}$
2^n explanations

Complexity of generating problem



Output P: $t_{total} = poly(\text{input} + \text{output})$

Incremental P: $t_p = poly(\text{input} + \sum_{i=1}^{p-1} |\alpha_i|)$

P delay: $t_p = poly(\text{Input})$

Slow
Fast

Prime implicate c of f

$f \models c,\ f \not\models c'$ for any $c' \subsetneq c$

Ex. $f = (x_1 \to x_2)(x_2 \to x_3)(x_3 \to x_1)$
$(mod(f) = \{(111), (000)\})$

- $\overline{x}_1 \vee x_2\ (\equiv x_1 \to x_2)$
  $f \models \overline{x}_1 \vee x_2,\ f \not\models \overline{x}_1,\ f \not\models x_2.$
- $\overline{x}_2 \vee x_1\ (\equiv x_2 \to x_1)$
  $f \models \overline{x}_2 \vee x_1,\ f \not\models \overline{x}_2,\ f \not\models x_1.$

Explanations and prime implicates

Explanation: minimal E s.t.
(1) $\varphi \cup E \models q \Leftrightarrow \varphi \models (\bigwedge_{x \in E} x \to q)$
(2) $\varphi \cup E$ is satisfiable

nontrivial explanation for q
⇕
prime implicate containing q

How to generate all prime implicates

$c_1 = (\bigvee_{x \in P(c_1)} x \vee \bigvee_{x \in N(c_1)} \overline{x})$
$c_2 = (\bigvee_{x \in P(c_2)} x \vee \bigvee_{x \in N(c_2)} \overline{x})$
$(P(c_1) \cap N(c_2) = \{z\}, N(c_1) \cap P(c_2) = \emptyset)$
resolvent
$c_3 = (\bigvee_{x \in (P(c_1) \setminus \{z\}) \cup P(c_2)} x \vee \bigvee_{x \in N(c_1) \cup (N(c_2) \setminus \{z\})} \overline{x})$

E.g., $(x_2 \vee \overline{x}_3 \vee \overline{x}_4)$: resolvent of
$(x_1 \vee \overline{x}_3 \vee \overline{x}_4)$ & $(\overline{x}_1 \vee x_2 \vee \overline{x}_3)$

$f \models c_1, c_2 \Rightarrow f \models c_3$

Procedure Resolution
Input: A CNF $\varphi = \bigwedge_{i=1}^{m} c_i$ representing f.
Output: All prime implicates of f.
Step 1: $S := \{c_i \mid i = 1, 2, \cdots, m\}$.
Step 2: Repeat (s) simplification and (r) resolution.
(s) Remove c from S if $\exists c^* \in S$ s.t. $c^* \models c$. $c^* \subsetneq c$
(r) Add a resolvent of two clauses in S.
Step 3: Output all clauses in S.

Ex. $\varphi = (\overline{x}_1 \vee \overline{x}_4)(\overline{x}_4 \vee \overline{x}_3)(\overline{x}_1 \vee x_2)(\overline{x}_3 \vee \overline{x}_5 \vee x_1)$
$S_0 = \{\overline{x}_1 \vee \overline{x}_4, \overline{x}_4 \vee \overline{x}_3, \overline{x}_1 \vee x_2, \overline{x}_3 \vee \overline{x}_5 \vee x_1\}$
$S_1 = S_0 \cup \{\overline{x}_3 \vee \overline{x}_5 \vee \overline{x}_4,\ \overline{x}_3 \vee \overline{x}_5 \vee x_2\}$
$S_2 = S_1 \setminus \{\overline{x}_3 \vee \overline{x}_5 \vee \overline{x}_4\}$

Prop. [Blake ('37), Brown ('68), Quine ('55), Samson-mills ('54)]
Resolution procedure generates all prime implicates.

Prop. Even if φ is Horn, resolution procedure may require exponential time.

Prop. There is no output P algorithm for generating all prime implicates, unless P=NP.

Procedure Resolution
Input: A CNF $\varphi = \bigwedge_{i=1}^{m} c_i$ representing f.
Output: All prime implicates of f.
Step 1: $S := \{c_i \mid i = 1, 2, \cdots, m\}$.
Step 2: Repeat (s) simplification and (r) resolution.
(s) Remove c from S if $\exists c^* \in S$ s.t. $c^* \models c$.
(r) Add a resolvent c_3 of two clauses c_1, c_2 in S.
Step 3: Output all clauses in S.

Modification
(1) Input resolution: $c_1 \in \varphi$
(2) Add a prime implicate c' s.t. $c' \models c_3$
(3) Output c' in (r) immediately, if c' is new.

Th. [Boros, Crama, Hammer ('90)]
If φ is Horn, then input-resolution procedure generates all prime implicates in incremental P time.

nontrivial explanation for q
⇕
prime implicate containing q

Procedure Resolution
Input: A CNF $\varphi = \bigwedge_{i=1}^{m} c_i$ representing f.
Output: All prime implicates of f.
Step 1: $S := \{c_i \mid i = 1, 2, \cdots, m\}$.
Step 2: Repeat (s) simplification and (r) resolution.
(s) Remove c from S if $\exists c^* \in S$ s.t. $c^* \models c$.
(r) Add a resolvent c_3 of two clauses c_1, c_2 in S.
Step 3: Output all clauses in S.

Modification
(1) Input resolution: $c_1 \in \varphi$
(2) Add a prime implicate c' s.t. $c' \models c_3$
(3) Output c' in (r) immediately, if c' is new.
(4) $c_2 \ni q$

Th. [Eiter, Makino (2002, 2003)]
All explanations for q from a Horn CNF can be computed with P delay.

Sketch: ▶

Cor. P many explanations for q from a Horn CNF can be computed in (input) P time.

Explanations for a negative literal

nontrivial explanation for a negative literal $\overline{q}$

⇕

prime implicate containing $\overline{q}$

Procedure Resolution

Input: A CNF $\varphi = \bigwedge_{i=1}^{m} c_i$ representing f.

Output: All prime implicates of f.

Step 1: $S := \{c_i \mid i = 1, 2, \cdots, m\}$.

Step 2: Repeat (s) simplification and (r) resolution.

(s) Remove c from S if $\exists c^* \in S$ s.t. $c^* \models c$.

(r) Add a resolvent c_3 of two clauses c_1, c_2 in S.

Step 3: Output all clauses in S.

Modification

(1) Input resolution: $c_1 \in \varphi$

(2) Add a prime implicate c' s.t. $c' \models c_3$

(3) Output c' in (r) immediately, if c' is new.

(4) ~~$c_2 \ni \overline{q}$~~ ⇒ $c_2 \ni \overline{q}$

Explanations for a negative literal

Prop. [Eiter, Makino (2003)]
Our resolution procedure does not generate all explanations for $\overline{q}$ from a Horn CNF.

Th. [Eiter, Makino (2003)]
There exists no output P algorithm for generating all explanations for $\overline{q}$ from a Horn CNF, unless P=NP.

Th. [Eiter, Makino (2003)]
All explanations for $\overline{q}$ from an acyclic Horn CNF can be computed in incremental P time.

Summary

Knowlege	Explanations E w.r.t. A=Lit	
	query q	query $\overline{q}$
Horn CNF	P delay	no output P
Acyclic Horn CNF	P delay	incremental P
Characteristic set	MDual	MDual

Knowlege	Explanations E w.r.t. $A \subseteq Lit$	
	query q	query $\overline{q}$
Horn CNF	coNPc	coNPc
Acyclic Horn CNF	coNPc	coNPc
Characteristic set	MDual	MDual

Model-based reasoning

Deduction $\varphi \models \psi$

⇕

$\varphi(v) = 1$ implies $\psi(v) = 1$

E.g., $\varphi = (\overline{x}_2 \vee \overline{x}_3 \vee x_4)(\overline{x}_3 \vee \overline{x}_4 \vee x_2)(\overline{x}_2 \vee \overline{x}_3 \vee x_1)$

$mod(\varphi) = \{(0000), (0001), (0010), (0100), (0101), (1000), (1001), (1010), (1100), (1101), (1111)\}$

All models $v \in mod(\varphi)$ satisfy $(x_3x_4 \to x_1)$

⇒ $\varphi \models (x_3x_4 \to x_1)$

$(0101) \in mod(\varphi)$ does not satisfy $(x_2x_4 \to x_1)$

⇒ $\varphi \not\models (x_2x_4 \to x_1)$

$|mod(\varphi)|$: large ⇒ inefficient

[P. N. Johnson-Laird ('83)].
Humans typically argue by just looking at some examples.

Some models $v \in mod(\varphi)$ satisfy $\psi(v) = 1$

⇒ conclude $\varphi \models \psi$; otherwise, $\varphi \not\models \psi$

Of course, incorrect !

$\exists S (\subseteq mod(\varphi))$ s.t.

$\forall v \in S$: $\psi(v) = 1$

⇕

$\forall v \in mod(\varphi)$: $\psi(v) = 1$ (i.e., $\varphi \models \psi$)

$v \wedge w$: intersection of $v, w \in \{0,1\}^n$

$(v \wedge w)_j = v_j \wedge w_j,\ j = 1, 2, \cdots, n$

E.g., $v = (1100)$, $v = (0110)$

$v \wedge w = (0100)$

Prop. [McKinsey ('43)]
f: a Horn function
$\Longleftrightarrow$ $mod(f)$ is closed under $\wedge$

Semantic, model theoretic characterization

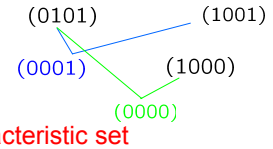
Horn CNF: syntactic characterization

Intersection closure

$$Cl_\wedge(T) = \{\bigwedge_{w \in S} w \mid \emptyset \neq S \subseteq T\}$$

E.g., $Cl_\wedge(\{(0101), (1001), (1000)\})$

$= \{(0101), (1001), (1000), (0001), (0000)\}$



Characteristic set

$$char(T) = \{v \in T \mid v \notin Cl_\wedge(T - \{v\})\}$$

$v \in char(T)$ for maximal model $v \in T$

Relational Database: generating set

Model-based representation of a Horn function

Given Characteristic set $char(T)$

Dedution: poly. time

Finding a nontrivial explanation E is poly. time.
Finding an explanation $E \subseteq A$ is poly. time.

Horn CNFs
Finding a nontrivial explanation E is poly. time.
Finding an explanation $E \subseteq A$ is NP-hard.

Summary

Knowlege	Explanations E w.r.t. $A = Lit$	
	query q	query $\overline{q}$
Horn CNF	P delay	no output P
Acyclic Horn CNF	P delay	incremental P
Characteristic set	MDual	MDual

Knowlege	Explanations E w.r.t. $A \subseteq Lit$	
	query q	query $\overline{q}$
Horn CNF	coNPc	coNPc
Acyclic Horn CNF	coNPc	coNPc
Characteristic set	MDual	MDual

Monotone Dualization

Input: A CNF φ of (a monotone function) f.
Output: Prime DNF ψ of f.

Ex. $\varphi = (x_1 \vee x_2)(x_2 \vee x_3)(x_3 \vee x_4)$

$\equiv \cancel{x_1x_2x_3} \vee \cancel{x_1x_2x_4} \vee x_1x_3 \vee \cancel{x_1x_3x_4} \vee \cdots$

$\equiv x_1x_3 \vee x_2x_3 \vee x_2x_4 \ = \ \psi$

Monotone Dualization

Input: A CNF φ of (a monotone function) f.
Output: Prime DNF ψ of f.

Many P equivalent problems

Polynomial？ OPEN

Bioch, Boros, Crama, Domingo, Eiter, Elbassioni, Fredman, Gaur, Gogic,Gottlob, Gunopulos, Gurvich, Hammer, Ibaraki, Johnson, Kameda, Kavvadias, Khachiyan, Khardon, Kogan, Krishnamurti, Lawler, Lenstra, Lovász, Mannila, Mishra, Papadimitriou, Pitt, Rinnoy Kan, Sideri, Stavropoulos, Tamaki, Toinonen, Uno, Yannakakis, ...

Polynomial？ OPEN

茨木俊秀．単調論理関数の同定問題とその複雑さ，
離散構造とアルゴリズム III,室田一雄（編）近代科学社，
pp. 1--33, 1994. Toshihide Ibaraki

Johnson. Open and closed problems in NP-completeness. Lecture given at the International School of Mathematics ``G. Stampacchia'': Summer School ``NP-Completeness: The First 20 Years'', Erice, Italy, June 20-27, 1991.

Lovasz. Combinatorial optimization: Some problems and trends, DIMACS Technical Report 92-53, 1992.

Papadimitriou. NP-completeness: A retrospective, In: Proc. 24th International Colloquium on Automata, Languages and Programming (ICALP), pp.2--6, Springer LNCS 1256, 1997.

Mannila. Local and Global Methods in Data Mining: Basic Techniques and Open Problems In: Proc. 29th ICALP, pp.57--68, Springer LNCS 2380, 2002.

Eiter, Gottlob. Hypergraph Transversal Computation and Related Problems in Logic and AI, In: Proc. European Conference on Logics in Artificial Intelligence (JELIA), pp. 549-564, Springer LNCS 2224, 2002

Best known

[Fredman, Khachiyan, 94]

$N^{o(\log N)}$ time where $N = |\varphi| + |\psi|$

[Eiter, Gottlob, Makino, 02]

$o(\log^2 N)$ guessed bits

Summary

Knowlege	Explanations E w.r.t. $A=Lit$ query q	query $\overline{q}$
Horn CNF	P delay	no output P
Acyclic Horn CNF	P delay	incremental P
Characteristic set	MDual	MDual

Knowlege	Explanations E w.r.t. $A \subseteq Lit$ query q	query $\overline{q}$
Horn CNF	coNPc	coNPc
Acyclic Horn CNF	coNPc	coNPc
Characteristic set	MDual	MDual

Explanations E w.r.t. $A=Lit$

Knowlege \ query	general	DNF	CNF	clause: pos	clause: Horn	clause: general	term: pos	term: neg	term: general
Horn CNF	coNPc	nOP	coNPc	Pd	coNPc	coNPc	Pd	nOP	nOP
char(Σ)	coNPc	nOP	coNPc	nOP	MD	nOP	MD	nOP	nOP

Explanations E w.r.t. $A \subseteq Lit$

Knowlege \ query	general	DNF	CNF	clause: pos	clause: Horn	clause: general	term: pos	term: neg	term: general
Horn CNF	Π_2^P	Π_2^P	coNPc		coNPc			coNPc	
char(Σ)	Π_2^P	Π_2^P	coNPc	nOP	MD	nOP	MD	coNPc	coNPc

nOP: no Output P, Pd: P delay, MD: Monotone Dual

Open Problems

1. Abductive Inference
2. Monotone Dualization
3. Horn Transformation
4. Vertex Enumeration

Conclusion

Generating abductive explanations from Horn CNFs

Practical side

High order logic, non-Horn case.

Procedure Resolution

Input: A CNF $\varphi = \bigwedge_{i=1}^{m} c_i$ representing f.

Output: All prime implicates of f.

Step 1: $S := \{c_i \mid i = 1, 2, \cdots, m\}$.

Step 2: Repeat (s) simplification and (r) resolution.

(s) Remove c from S if $\exists c^* \in S$ s.t. $c^* \models c$.

(r) Add a resolvent c_3 of two clauses c_1, c_2 in S.

Step 3: Output all clauses in S.

Modification

(1) Input resolution: $c_1 \in \varphi$

(2) Add a prime implicate c' s.t. $c' \models c_3$

(3) Output c' in (r) immediately, if c' is new.

(4) $c_2 \ni q$

Sketch: All explanations can be generated by the input resolution procedure if φ is definite Horn

prime

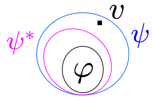
No negative clause $(\overline{x}_1 \vee \overline{x}_3 \vee \overline{x}_2)$

ψ^*: CNF consisting of all prime implicates $\ni q$

ψ: CNF consisting of all prime implicates $\ni q$ generated so far

Note ψ^*: irredundant ($\forall c \in \varphi^* : \psi^* \not\equiv \psi^* \setminus \{c\}$)

if $\psi \neq \psi^*$ $\quad \exists v : \psi(v) = 1, \psi^*(v) = 0$



v: maximal

$\exists c \in \varphi, \exists c' \in \psi^* \setminus \psi : c(v) = c'(v) = 0$

$v = (0, 0, \ldots, 0, 1, \ldots, 1)$ (q, p under the first two entries; N', N over the last block)

$c = (p \vee \bigvee_{x \in N} \overline{x})$

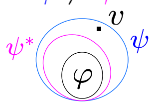
$c' = (q \vee \bigvee_{x \in N'} \overline{x})$

$p \neq q$

ψ^*: CNF consisting of all prime implicates $\ni q$

ψ: CNF consisting of all prime implicates $\ni q$ generated so far

if $\psi \neq \psi^*$ $\quad \exists v : \psi(v) = 1, \psi^*(v) = 0$



v: maximal

$\exists c \in \varphi, \exists c' \in \psi^* \setminus \psi : c(v) = c'(v) = 0$

$v = (0, 0, \ldots, 0, 1, \ldots, 1)$ (q, p under the first two entries; N', N over the last block)

$c = (p \vee \bigvee_{x \in N} \overline{x})$

$c' = (q \vee \bigvee_{x \in N'} \overline{x})$

$v + e_p = (0, 1, \ldots, 0, 1, \ldots, 1)$

$c'(v+e_p) = 0, \ \psi^*(v+e_p) = 0, \ \psi(v+e_p) = 0$

$\exists c'' \in \psi : c''(v+e_p) = 0$

Since $c''(v) = 1, \ c'' = (q \vee \bigvee_{x \in N'' \cup \{p\}} \overline{x})$

Resolution of c and c''

Proof. ($mod(f)$ is closed under $\bigwedge$)

$v = (1 \cdots 1 \mid 1 \cdots 1 \mid 0 \cdots 0 \mid 0 \cdots 0)$ (blocks I_1, I_2, I_3, I_4)

$w = (1 \cdots 1 \mid 0 \cdots 0 \mid 1 \cdots 1 \mid 0 \cdots 0)$

$v \wedge w = (1 \cdots 1 \mid 0 \cdots 0 \mid 0 \cdots 0 \mid 0 \cdots 0)$

$\exists$ Horn clause $c = \bigwedge_{i \in N} \overline{x}_i \wedge x_j$:

$c(v) = c(w) = 1, \ c(v \wedge w) = 0$

From $c(v \wedge w) = 0, \ N \subseteq I_1, \ j \in I_2 \cup I_3 \cup I_4$

$c(v) = 0$ or $c(w) = 0$. a contradiction.

Metric Labeling: Upper and Lower Bounds

SEFFI NAOR

COMPUTER SCIENCE DEPT.
TECHNION
HAIFA, ISRAEL

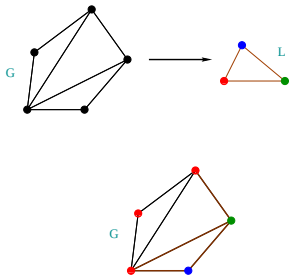
Based on Joint Work with:
CHANDRA CHEKURI, JULIA CHUZHOY, SANJEEV KHANNA, ROY SCHWARTZ, AND LEONID ZOSIN.

Metric Labeling: The Problem

- **Input:**
  - Undirected graph G with edge weights $w(u\ v)$.
  - A set L of k labels equipped with a metric d.
  - Cost function $c : V(G) \times L \to \mathcal{R}$.
- **Goal:** An assignment $f : V(G) \to L$ (or a labeling of $V(G)$).
- **Objective Function:** minimize

$$\underbrace{\sum_{u \in V(G)} c(u\ f(u))}_{\text{Labeling Cost}} + \underbrace{\sum_{u\ v} w(u\ v) d(f(u)\ f(v))}_{\text{Separation Cost}}$$

Example



Combinatorial Optimization: Related Problems

- **Multiway Cut:**
  - Set of terminals t_1 t_k.
  - Find minimum cut separating the terminals.
  - Special case of ML: uniform metric and no assignment cost.
- **0-Extension:**
  - Same as multiway cut except that metric is arbitrary: penalty of cut edge depends on terminals that endpoints belong to.
  - Special case of ML.
- **Quadratic Assignment:** dropping the bijective property in QA yields metric labeling.

Motivation

- Clean and general abstraction of classification problems [Kleinberg and Tardos, 1999].
- Links to Markov random fields and their applications.
- Specific applications to image processing and analysis.
- Generalization of well known optimization problems.

Do assignment costs matter?

The $(0\ \infty)$-Extension Problem:

$c(u\ i) \in \{0\ \infty\}$ for all $u \in V(G)\ 1 \le i \le k$.

- Approximation preserving reduction from metric labeling with arbitrary assignment costs to $(0\ \infty)$-extension.
- Reduction preserves label set, but changes graph (in a simple way).

Theorem. [Chuzhoy 2001] *If there is a $f(n\ k)$-approximation algorithm for $(0\ \infty)$-extension, then there is a $f(n{+}nk\ k)$-approximation algorithm for general metric labeling.*

Relaxation: Embedding in a Simplex

[Chekuri, Khanna, N., Zosin, 2001]

- For each $v \in V$: $v \longmapsto (x(v\ 1)\ x(v\ 2) \quad x(v\ k))$, where

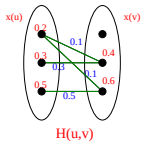
$$\sum_{i=1}^{k} x(v\ i) = 1$$

Vertex v is mapped into a probability distribution over the label set.

- Distance between u and v defined by Earthmover Metric - solution to a transportation problem between $(u\ 1) \quad (u\ k)$ and $(v\ 1) \quad (v\ k)$ with respect to label metric d.

$$d_{EM}(u\ v) = \sum_{i\ j} d(i\ j) \cdot x(u\ i\ v\ j)$$

$x(u\ i\ v\ j)$ - flow on edge $((u\ i)\ (v\ j))$



Linear Program: Computing the Embedding

- **Result:** Embedding in a simplex where distances are defined by an earthmover metric (and not ℓ_1).
- **Objective Function:** Minimize

$$\underbrace{\sum_{u \in V} \sum_{i=1}^{k} c(u\ i) \cdot x(u\ i)}_{\text{labeling cost}} + \underbrace{\sum_{(u\ v) \in E} w(u\ v) \sum_{1 \le i\ j \le k} d(i\ j) \cdot x(u\ i\ v\ j)}_{\text{separation cost}}$$

Constraints

$$\sum_{i=1}^{k} x(u\ i) = 1 \quad \forall\ u \in V$$

$$\sum_{j=1}^{k} x(u\ i\ v\ j) - x(u\ i) = 0 \quad \forall\ u\ v \in V\ i \in 1 \quad k$$

$$x(u\ i\ v\ j) - x(v\ j\ u\ i) = 0 \quad \forall\ u\ v \in V, i\ j \in 1 \quad k$$

$$x(u\ i)\ x(u\ i\ v\ j) \ge 0$$

Uniform Metric

- For any $i \neq j$, $d(i\ j) = 1$.
- What does the earthmover solution look like? for edge $(u\ v)$:

$$x(u\ i\ v\ i) = \min\{x(u\ i)\ x(v\ i)\}$$

- Thus,

$$d_{EM}(u\ v) = \sum_{i\ j} d(i\ j) x(u\ i\ v\ j) \ge \frac{1}{2} \cdot \sum_{i=1}^{k} |x(u\ i) - x(v\ i)|$$

Uniform Metric: Rounding Algorithm

Rounding an LP solution. [Kleinberg and Tardos, 1999].

Idea: Random choices should be correlated.

Algorithm: repeat until all vertices are labeled.

1. pick i at random from $\{1\ 2 \quad k\}$.
2. pick θ at random from the interval $[0\ 1]$.
3. label an unlabeled vertex u with i iff $\theta \le x(u\ i)$.

Uniform Metric: Integrality Gap

Observation: Probability of assigning i to u is exactly $x(u\ i)$.

Lemma: Probability that u and v get different labels is at most

$$\sum_{i=1}^{k} |x(u\ i) - x(v\ i)|$$

Recall: $d_{EM}(u\ v) \geq \frac{1}{2} \cdot \sum_{i=1}^{k} |x(u\ i) - x(v\ i)|$

Theorem: For a uniform metric, integrality gap ≤ 2.

Open Question: Can the 2-approximation be improved?

General Metrics

- Solve the simplex embedding LP.
- Approximate the fractional solution to the LP by a deterministic HST metric losing a factor of $O(\log k)$.
- The integrality gap on an HST tree is $O(1)$.
- Yielding an $O(\log k)$-approximation for general metrics [Kleinberg and Tardos, 1999].

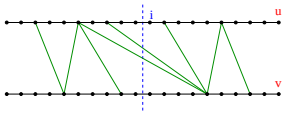
Linear Metric

Rounding of LP solution:

- Assume w.l.o.g. labels are integers $1\ 2 \quad k$.
- For each vertex u, define $\alpha(u\ i) = \sum_{j=1}^{i} x(u\ j)$.
- Pick θ uniformly at random from $[0\ 1]$.
- $L(u) = i$ iff $\alpha(u\ i-1) < \theta \leq \alpha(u\ i)$.
- All vertices get a label since $\alpha(u\ k) = 1$.

Lemma 1: $d_{EM}(u\ v) \geq \sum_{i=1}^{k} |\alpha(u\ i) - \alpha(v\ i)|$.

Flow is uncrossing



Flow crossing i is exactly $|\alpha(u\ i) - \alpha(v\ i)|$. □

Analysis

Lemma 1: $d_{EM}(u\ v) \geq \sum_{i=1}^{k} |\alpha(u\ i) - \alpha(v\ i)|$

Lemma 2: $\mathbf{E}[d((L(u)\ L(v))] = \sum_{i=1}^{k} |\alpha(u\ i) - \alpha(v\ i)|$

$\Downarrow$

Theorem: The integrality gap of the LP for the line metric is 1.

Convex functions on the line

- $d(i\ j) = f(|i-j|)$ where f is convex and increasing.
- d is a metric iff f is *linear*.
- The linear programming formulation is useful for convex f.
- Integrality gap is 1 since flow is uncrossing.

Truncated Linear Metric

- $d(i\ j) = \min\{M\ |i-j|\}$.
- Applications to image processing.
- Generalizes uniform and linear metrics and is NP-hard.
- $2+\sqrt{2} \simeq 3\ 414$-approximation by generalizing the linear algorithm. [Chekuri, Khanna, N., Zosin, 2001]
- **Open Question**: Improve the approximation factor.

Truncated Quadratic Distance

- $d(i\ j) = \min\{(i-j)^2\ M\}$. Not a metric!
- Useful function for vision applications.
- $O(\sqrt{M})$-approximation easy.
- **Open Questions:**
  - NP-hard?
  - LP gap?
  - $O(1)$ approximation?

0-Extension Problem

- **Input:**
  - Graph G with edge weights $w(u\ v)$.
  - $T \subset V(G)$ - Set of k terminals.
  - d - Metric on T.
- **Solution**: Partitioning of the graph, s.t. each terminal is in a different connected component.
  - $t(v)$ - terminal in connected component of v.
- **Objective**: minimize $\sum_{(u\ v)\in E(G)} w(u\ v) \cdot d(t(u)\ t(v))$.

0-Extension Problem: Open Questions

- Is 0-extension easier than $(0\ \infty)$-extension?
- I.e., if each non-terminal vertex can be labeled for free, does that make the metric labeling problem easier?
- Best approximation factor known: $O\left(\frac{\log k}{\log\log k}\right)$ [FHRT] for general metrics (improving a previous factor of $O(\log k)$ [CKR]).

Balanced Metric Labeling

- **Input:** Metric labeling instance.
- **Additional constraint:**

  Each label can be assigned to at most ℓ vertices.

  [N., Schwartz, STOC 2005]

Motivation

- Minimum weight k-way balanced partitioning:
  - Each part contains at most $2n/k$ vertices.
  - Minimizing weight of edge cuts.
- Special case of balanced metric labeling:
  - Label is equivalent to a Part.
  - $\ell \leq 2n/k$.
  - Uniform metric.

Motivation (contd.)

- What if each vertex can only be labeled by a subset of the labels?
  - The balanced $\{0\ \infty\}$-extension problem.
- Application: Clustering Base Transceiver Stations in GSM networks:
  - Weighted graph on the BTS-s: traffic $\mapsto$ edge weight.
  - Each cluster is controlled by a Base Station Controller (= label).
  - Base Station Controller have bounded capacity.
  - Each BTS can only be assigned to a subset of the BSC-s.
- Graph arrangement problems:
  - E.g., linear-arrangement: linear metric and capacity = 1.

Balanced Uniform Metric Labeling - Difficulties

- Bounding the number of vertices assigned to each label?
  - Not obvious in the methods developed for uncapacitated uniform metric labeling, e.g., the Kleinberg-Tardos algorithm.
- Incorporating label assignment costs?
  - Not obvious in the techniques developed for approximating graph partitioning problems ([LR], [ENRS], and [ARV]).
  - For example, there may not always exist a label that can be assigned to all vertices in a single cluster of the partition.

Spreading Constraints

- Very useful for approximating graph partitioning problems.
- Example: $\forall S \subseteq V\ \forall u \in S$: $\sum_{v \in S} d(u\ v) \geq |S| - \ell$
- For large subsets S, there is a radius guarantee:

$$\exists v \in S:\ d(u\ v) \geq 1 - \frac{\ell}{|S|}$$

- Radius guarantee $\Rightarrow$ Ball growing techniques can be applied.

The Relaxation

- Embedding in a k-dimensional simplex.
- Spreading constraints.
- Capacity constraints:

$$\forall \text{ label } j: \quad \sum_{v \in V} x(v\ j) \leq \ell$$

- Closeness constraints.

The Relaxation: Closeness Constraints

- Closeness of u and v wrt label j: $c_j(u\ v) \leq x(u\ j)\ x(v\ j)$.
- Variation distance: $\forall u\ v$,

$$d(u\ v) = 1 - \sum_{j \in L} c_j(u\ v)$$

- Triangle inequality: $\forall u\ v\ w \in V$,

$$\sum_j |c_j(u\ v) - c_j(u\ w)| \leq 1 - \sum_j c_j(v\ w)$$

The Approximation Algorithm

- **Overview:** A combination of randomized metric decomposition and label assignment techniques.
- **Initial Labeling:** Each vertex v is assigned a root labeling, $f^* : V \to L$, satisfying:

$$\mathbb{P}\mathrm{r}[f^*(v) = j] = x(v\ j) \qquad \forall v \in V\ \forall \text{ label } j$$

- **Iteratively:** Each vertex, in its turn, is a root and labels a subset of the unlabeled vertices.

Radius and Label Tests

- **Current root:** Vertex u.
- **Radius test:**
  - Choose radius R from the distribution:

$$f_R(r) = \left(\frac{n}{n-1}\right) \cdot \frac{1+\varepsilon}{\varepsilon} \cdot \ln n \cdot n^{-r \cdot \frac{1+\varepsilon}{\varepsilon}} \quad r \in \left[0 \ \frac{\varepsilon}{1+\varepsilon}\right]$$

  - Define a ball of radius R, with respect to metric d, around root vertex u:

$$\{x \mid d(u\ x) \leq R\}$$

Radius and Label Tests (contd.)

- **Label Test:**
  - Choose uniformly in random $\alpha \in [0\ x(u\ f^*(u))]$.
  - Define vertices close to the root u with respect to root label $f^*(u)$:

$$\{x \mid c_{f^*(u)}(u\ x) \geq \alpha\}$$

- **Labeling:** All unlabeled vertices that pass both radius and label tests receive label $f^*(u)$.

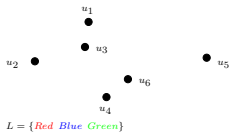
Approximation Algorithm: Summary

- For each $u \in V$, iteratively:
  - Apply radius and label test.
- Output labeling.

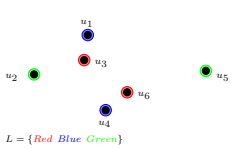
Theorem: Upon termination, all vertices are labeled.

Proof: Each vertex passes the radius and label tests when it becomes the root vertex.

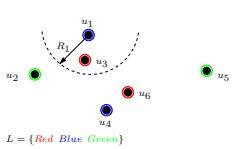
The Approximation Algorithm - Example



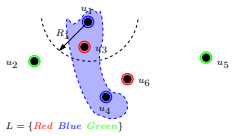
The Approximation Algorithm - Example



The Approximation Algorithm - Example

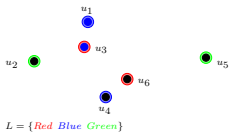


The Approximation Algorithm - Example



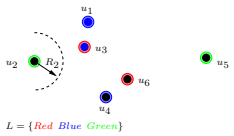
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



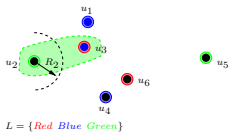
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



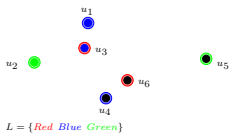
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



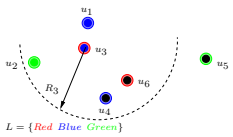
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



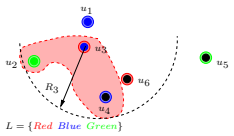
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



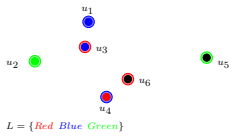
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



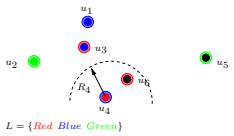
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



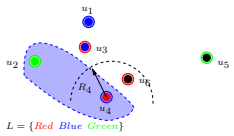
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



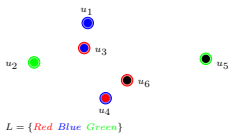
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



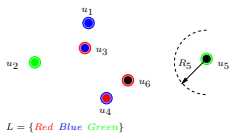
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



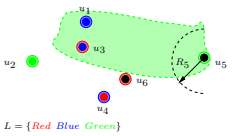
$L = \{Red\ Blue\ Green\}$

The Approximation Algorithm - Example



$L = \{Red\ Blue\ Green\}$

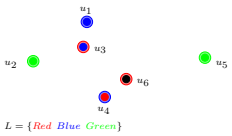
The Approximation Algorithm - Example



$L = \{Red\ Blue\ Green\}$

48

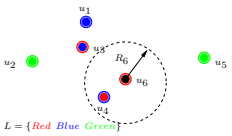
The Approximation Algorithm - Example



$L = \{Red\ Blue\ Green\}$

49

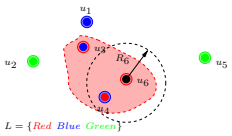
The Approximation Algorithm - Example



$L = \{Red\ Blue\ Green\}$

50

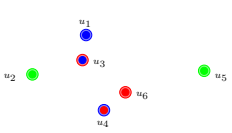
The Approximation Algorithm - Example



$L = \{Red\ Blue\ Green\}$

51

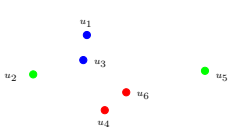
The Approximation Algorithm - Example



$L = \{Red\ Blue\ Green\}$

52

The Approximation Algorithm - Example



$L = \{Red\ Blue\ Green\}$

53

Analysis

- **Difficulty:**
  - Capacity: Easy to bound the number of vertices assigned to a label with independent random labels.
  - Vertex separation costs: If the labels chosen for the vertices are dependent [KT], cost of vertex separation is bounded.

54

Analysis (contd.)

- **Main Ingredient:** The algorithm balances the dependencies between the labels assigned to the vertices.
  - Label of a vertex depends on only a limited number of other labels: Labels of vertices that are far from each other are independent.
  - Spreading constraints: not too many vertices are close.
  - Number of vertices assigned to each label is bounded via a new inequality of Janson for tail bounds of (partly) dependent random variables.
  - Separation cost is bounded.

55

Approximation Factor

- Bicriteria approximation factor: For any $0 < \varepsilon < 1$,
  - $O\left(\frac{\ln n}{\varepsilon}\right)$-approximation to the solution cost.
  - $\min\left\{\frac{O(\ln k)}{1-\varepsilon}\ \ell + 1\right\}(1+\varepsilon)\,\ell$ vertices are assigned to each label.
- For $\ell = O(1)$ or $k = O(1)$, capacity is violated by a constant multiplicative deviation.
- Compare with balanced k-way partitioning:

  Either $(O(\log n)\ \text{const})$, [ENRS] or $(O(\sqrt{\log n}\log k)\ \text{const})$ [ARV].

56

Open Questions

- Can we improve the approximation factor?
- Can we obtain the same biciriteria factor $(\log n\ \text{constant})$ known for balanced partitioning?

57

Hardness of Metric Labeling

- Back to uncapacitated metric labeling [Chuzhoy, N., FOCS 2004]:
- There is no constant approximation for Metric Labeling unless P=NP.
- No $\log^{\frac{1}{2}-\delta} n$-approximation exists unless NP $\subseteq$ DTIME$(n^{\text{poly}\log n})$ (for any constant δ).
- Hardness is proved for $(0\ \infty)$-extension.

58

Gap 3SAT(5)

Input: A 3SAT(5) formula φ on n variables.

- φ is a YES-instance if it is satisfiable.
- φ is a NO-instance (with respect to some ε) if at most a $(1-\varepsilon)$-fraction of the clauses are simultaneously satisfiable.

Theorem: [ALMSS'92] There is some $0 < \varepsilon < 1$, such that it is NP-hard to distinguish between YES and NO instances.

59

A 2-prover Protocol for 3SAT(5) Formula φ

- Verifier: randomly chooses clause C and one of its variables x.
- Prover 1: receives the clause C and answers with an assignment to the variables of C that satisfy it.
- Prover 2: receives variable x and answers with an assignment to x.
- Verifier: checks that the two assignments match.

Theorem:
• If φ is a YES-instance: there is a strategy of the provers such that the verifier always accepts.
• If φ is a NO-instance: for any strategy, the acceptance probability is at most $(1 - \frac{\varepsilon}{3})$.

The Raz Verifier

- Performs ℓ parallel repetitions of the 2-Prover Protocol.
- A query to prover 1 is an ℓ-tuple of clauses and a query to prover 2 is an ℓ-tuple of variables.
- If φ is a YES-instance: then there is a strategy of the two provers that makes the verifier always accept.
- If φ is a NO-instance: then for any strategy of the two provers the acceptance probability is at most $2^{-O(\ell)}$.

A Simple $(3 - \varepsilon)$-Hardness

- Start from a 3SAT(5) formula φ.
- Use the Raz verifier with ℓ repetitions (ℓ is a large constant) to produce a $(0\ \infty)$-extension instance:
  - If φ is a YES-instance, then there is a solution of cost $|R|$.
  - If φ is a NO-instance, then the cost of any solution is at least $(3 - \delta)|R|$.

A $(3 - \varepsilon)$-Hardness: Label Set

- $\forall$ query-answer pair $(q\ a)$ of each prover, there is a label $\ell(q\ a)$.
- Given:
  - random string r.
  - queries q_1, q_2 sent to the provers under r.
  - a_1 and a_2 is a pair of consistent answers to q_1 and q_2.

  $\Longrightarrow$ There is an edge of length 1 between $(q_1\ a_1)$ and $(q_2\ a_2)$.
- Label distances are defined by shortest paths in the label graph.
- Label graph is bipartite: Part $\Leftrightarrow$ Prover. Distances: either 1, or ≥ 3.

A $(3 - \varepsilon)$-Hardness: the Graph

- For each possible query q to provers 1 and 2 there is a vertex $v(q)$ that can only be assigned to its corresponding labels ($\ell(q\ a)$).
- For each random string r, let q_1, q_2 be the queries sent to the two provers under r. There is an edge between $v(q_1)$ and $v(q_2)$.

Note that every assignment of the vertices to the labels defines a strategy for the provers and vice versa.

Properties

- If φ is a YES-instance:
  - $\exists$ strategy of provers s.t. their answers are always consistent.
  - Strategy defines an assignment of vertices to labels of cost $|R|$.
- If φ is a NO-instance:
  - Assignment of labels to vertices defines a strategy for the provers.
  - Acceptance probability of this strategy is at most $2^{-O(\ell)}$.
  - Hence, almost all the edges in the graph pay (at least) 3.
  - The solution cost is arbitrarily close to $3|R|$.

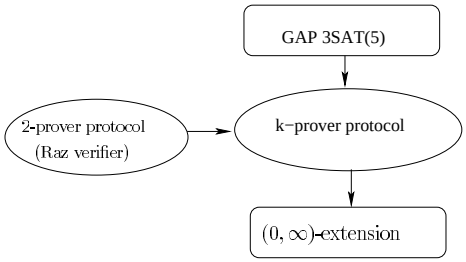
Extending to $\sqrt{\log n}$-Hardness

Difficulty:

- Suppose queries q_1 and q_2 are sent to the two provers.
- If their answers a_1,a_2 are inconsistent, then there is a path of length (precisely) 3 in the label graph between the labels $\ell(q_1\ a_1)$ and $\ell(q_2\ a_2)$.
- This is true even if the answers are inconsistent in many coordinates.

Goal: If the answers are inconsistent in many coordinates, the length of the path between them should also be large.

Plan



A New k-Prover System

For each pair of provers $(i\ j)$, $1 \le i < j \le k$:

- The verifier chooses randomly and independently clause C_{ij} and one of its variables x_{ij}.
- Prover i receives clause C_{ij} and answers with an assignment to its variables satisfying the clause.
- Prover j receives x_{ij} and answers with an assignment to it.
- Every other prover $a \neq i\ j$ receives both C_{ij} and x_{ij} and answers with an assignment to the variables of C_{ij} satisfying the clause.

A Query

Each query has $\binom{k}{2}$ coordinates.

Coordinate $(a\ b)$ (for $a < b$) of the query for prover i:

- If $i = a$, it contains C_{ab}
- If $i = b$, it contains x_{ab}
- If $a\ b \neq i$, it contains both C_{ab} and x_{ab}

Example: Queries in a 3-Prover Protocol

	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$
P_1	$C_{1\,2}$	$C_{1\,3}$	$C_{2\,3}\ x_{2\,3}$
P_2	$x_{1\,2}$	$C_{1\,3}\ x_{1\,3}$	$C_{2\,3}$
P_3	$C_{1\,2}\ x_{1\,2}$	$x_{1\,3}$	$x_{2\,3}$

The k-Prover System: Properties

Definition:

- Let A_i, A_j be the answers of provers i, j to their queries.
- The answers are weakly consistent if their $(i\ j)$ coordinates match.
- They are strongly consistent if all their coordinates match.

Theorem: If φ is a YES-instance, then there is some strategy of the provers, such that their answers are always strongly consistent.

Theorem: If φ is a NO-instance, then for every pair of provers, the probability that their answers are weakly consistent is at most $(1 - \frac{\varepsilon}{3})$.

The Reduction - an Overview

Given a 3SAT(5) formula φ on n variables, we use the k-prover system to produce an instance of $(0\ \infty)$-extension, such that:

- If φ is a YES-instance, there is a solution of cost $\frac{k}{2}|R|$.
- If φ is a NO-instance, the cost of any solution is at least $|T| \geq \binom{k}{2}\frac{\varepsilon}{3}|R|)$
- Thus, the gap between YES and NO instances is $\Omega(k)$.
- The instance size is $N = n^{O(k^2)}$.

$\Rightarrow$ Choosing $k = \text{poly}(\log n)$, no $\log^{\frac{1}{2}-\delta} N$ approximation exists unless NP $\subseteq$ DTIME$(n^{\text{poly}\log n})$ (for any constant δ).

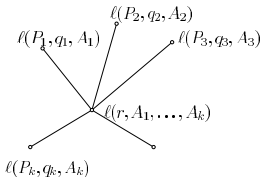
The Construction: Label Metric

There are two types of labels:

- Query Label $\ell(P_i\ q_i\ A_i)$:
  - For each prover P_i,
  - For each query q_i to prover P_i,
  - For each possible answer A_i to q_i.
- Constraint Label $\ell(r\ A_1 \quad A_k)$:
  - For each random string r,
  - For each k-tuple $A_1 \quad A_k$ of strongly consistent answers of the provers to the queries implied by r.

Label Metric: Edges

Let r be a random string, $q_1 \quad q_k$ be the corresponding queries, and let $A_1 \quad A_k$ be a k-tuple of strongly consistent assignments. For each i, there is an edge of length $\frac{1}{2}$ between $\ell(r\ A_1 \quad A_k)$ and $\ell(P_i\ q_i\ A_i)$.



The Graph: Vertices

- Query Vertices: For each prover P_i, for each query q_i to P_i, there is a vertex $v(P_i\ q_i)$, which can only be assigned to labels corresponding to the same query of the same prover (i.e., $\ell(P_i\ q_i\ A)$.)

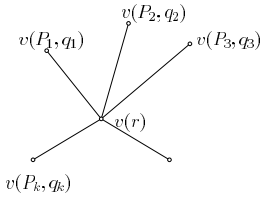
  Note that the assignments of all the query vertices to the labels define a strategy of the k provers.

- Constraint Vertices: For each random string r, there is a vertex $v(r)$, which can be only assigned to the labels corresponding to r (i.e., $\ell(r\ A_1 \quad A_k)$).

  Note that the assignment of $v(r)$ defines the answers of the provers when the random string is r.

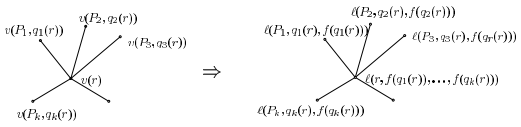
The Graph: Edges

Let $q_1 \quad q_k$ be the queries corresponding to random string r. Then, for each i, there is an edge between $v(r)$ and $v(P_i\ q_i)$.



YES Instance

- There exists an accepting strategy of the provers.
- Queries $q_1 \quad q_k$ correspond to random string r.
- $A_1 \quad A_k$ are the answers to the queries.



Therefore, the solution cost is $\frac{k}{2}|R|$.

NO Instance

- Assignments of the query vertices define a strategy for the provers.
- Let T be the set of "inconsistent" triples $(r\ i\ j)$ ($i < j$), s.t. for random string r, the answers of provers i and j are not weakly consistent.
- $|T| \geq \binom{k}{2}\frac{\varepsilon}{3}|R|$. (Recall that the probability that a pair is weakly consistent is at most $(1 - \frac{\varepsilon}{3})$).
- We can show that the solution cost is at least $|T|$, yielding a gap of $\Omega(k)$ between YES and NO instances.
- Since the construction size is $N = n^{O(k^2)}$, choosing $k = \text{poly}(\log n)$, no $\log^{\frac{1}{2}-\delta} N$ approximation exists unless NP $\subseteq$ DTIME($n^{\text{poly}\log n}$) (for any constant δ).

78

Open Questions

- There is still a gap between the logarithmic upper bound and the lower bound of $\log^{1/2-\delta} n$ on the approximability of metric labeling. Can this gap be closed?
- Can we prove better (non-constant?) lower bounds on the approximability of 0-Extension?
- Or, can we obtain better approximation factors?

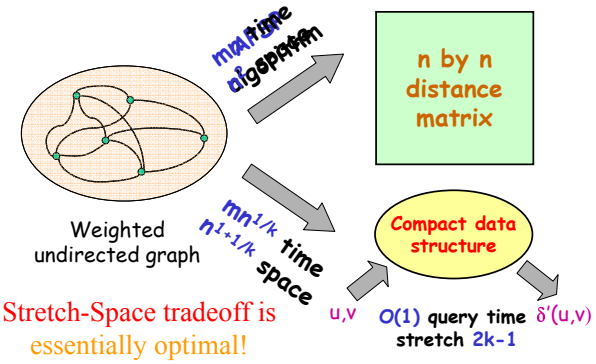
79

Approximate Distance Oracles
and
Spanners with sublinear surplus

Mikkel Thorup
AT&T Research

Uri Zwick
Tel Aviv University

Approximate Distance Oracles (TZ'01)



Stretch-Space tradeoff is essentially optimal!

Approximate Shortest Paths

Let $\delta(u,v)$ be the distance from u to v.

Multiplicative error

An estimated distance $\delta'(u,v)$ is of stretch t iff

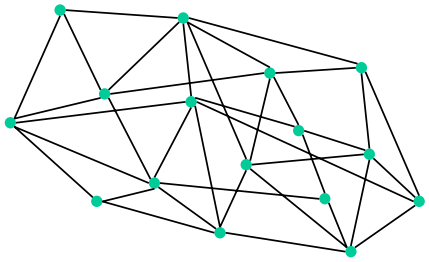
$$\delta(u,v) \le \delta'(u,v) \le t \cdot \delta(u,v)$$

Additive error

An estimated distance $\delta'(u,v)$ is of surplus t iff

$$\delta(u,v) \le \delta'(u,v) \le \delta(u,v) + t$$

Spanners



Given an **arbitrary** dense graph, can we always find a relatively **sparse subgraph** that approximates **all** distances fairly well?

Spanners [PU'89,PS'89]

Let $G=(V,E)$ be a weighted undirected graph.

A subgraph $G'=(V,E')$ of G is said to be a t-spanner of G iff $\delta_{G'}(u,v) \le t\,\delta_G(u,v)$ for every u,v in V.

Theorem:
Every weighted undirected graph has a $(2k-1)$-spanner of size $O(n^{1+1/k})$. [ADDJS '93]
Furthermore, such spanners can be constructed deterministically in linear time. [BS '04] [TZ '04]

The size-stretch trade-off is essentially optimal.
(Assuming there are graphs with $\Omega(n^{1+1/k})$ edges of girth 2k+2, as conjectured by Erdös and others.)

Additive Spanners

Let $G=(V,E)$ be a unweighted undirected graph.

A subgraph $G'=(V,E')$ of G is said to be an additive t-spanner if G iff $\delta_{G'}(u,v) \le \delta_G(u,v)+t$ for every $u,v \in V$.

Theorem: Every unweighted undirected graph has an additive 2-spanner of size $O(n^{3/2})$. [ACIM '96] [DHZ '96]

Theorem: Every unweighted undirected graph has an additive 6-spanner of size $O(n^{4/3})$. [BKMP '04]

Major open problem

Do all graphs have additive spanners with only $O(n^{1+\varepsilon})$ edges, for every $\varepsilon>0$?

Spanners with sublinear surplus

Theorem:

For every $k>1$, every undirected graph $G=(V,E)$ on n vertices has a subgraph $G'=(V,E')$ with $O(n^{1+1/k})$ edges such that for every $u,v \in V$, if $\delta_G(u,v)=d$, then $\delta_{G'}(u,v)=d+O(d^{1-1/(k-1)})$.

$d \Rightarrow d+O(d^{1-1/(k-1)})$

Extends and simplifies a result of Elkin and Peleg (2001)

All sorts of spanners

A subgraph $G'=(V,E')$ of G is said to be a functional f-spanner if G iff $\delta_{G'}(u,v) \le f(\delta_G(u,v))$ for every $u,v \in V$.

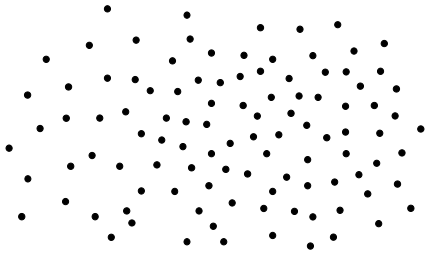
size	$f(d)$	reference
$n^{1+1/k}$	$(2k-1)d$	[ADDJS '93]
$n^{3/2}$	$d+2$	[ACIM '96] [DHZ '96]
$n^{4/3}$	$d+6$	[BKMP '04]
$\beta n^{1+\delta}$	$(1+\varepsilon)d+\beta(\varepsilon,\delta)$	[EP '01]
$n^{1+1/k}$	$d+O(d^{1-1/(k-1)})$	[TZ '05]

Part I

Approximate Distance Oracles

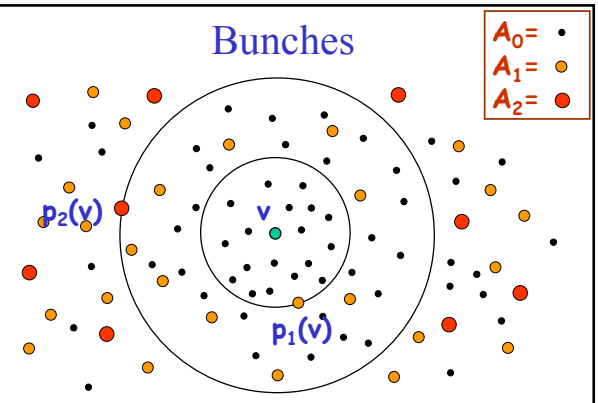
Approximate Distance Oracles [TZ'01]

A hierarchy of centers



$A_0 \leftarrow V$; $A_k \leftarrow \varnothing$;
$A_i \leftarrow \text{sample}(A_{i-1}, n^{-1/k})$;

Bunches



$$B(v) \leftarrow \bigcup_i \{w \in A_i - A_{i+1} \mid \delta(w,v) < \delta(A_{i+1},v)\}$$

Lemma: $E[|B(v)|] \le kn^{1/k}$

Proof: $|B(v) \cap A_i|$ is stochastically dominated by a geometric random variable with parameter $p=n^{-1/k}$.

The data structure

Keep for every vertex $v \in V$:

- The centers $p_1(v), p_2(v), \ldots, p_{k-1}(v)$
- A **hash table** holding $B(v)$

For every $w \in V$, we can check, in **constant time**, whether $w \in B(v)$, and if so, what is $\delta(v,w)$.

Query answering algorithm

Algorithm $\text{dist}_k(u,v)$

$w \leftarrow u$, $i \leftarrow 0$

while $w \notin B(v)$

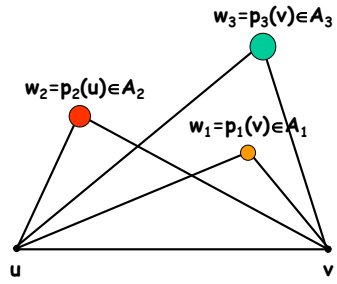
{ $i \leftarrow i+1$

$(u,v) \leftarrow (v,u)$

$w \leftarrow p_i(u)$ }

return $\delta(u,w) + \delta(w,v)$

Query answering algorithm



Analysis

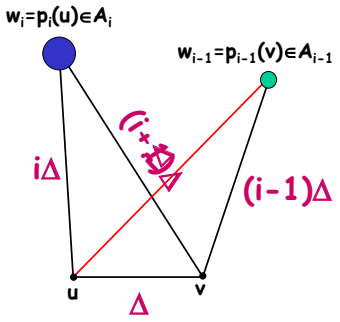
Claim 1:

$\delta(u,w_i) \le i\Delta$, i even

$\delta(v,w_i) \le i\Delta$, i odd

Claim 2:

$\delta(u,w_i) + \delta(w_i,v) \le (2i+1)\Delta \le (2k-1)\Delta$

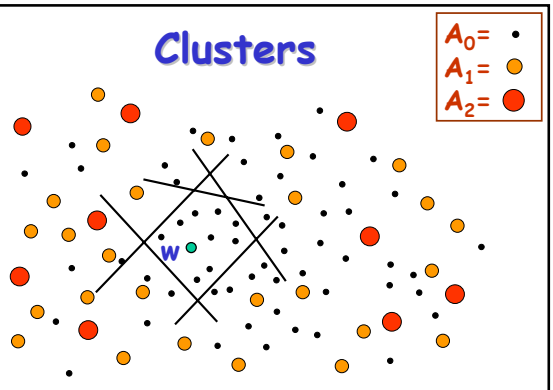


Where are the spanners?

Define clusters, the "dual" of bunches.

For every $u \in V$, include in the spanner a tree of shortest paths from u to all the vertices in the cluster of u.

Clusters



$C(w) \leftarrow \{v \in V \mid \delta(w,v) < \delta(A_{i+1},v)\}$, $w \in A_i - A_{i+1}$

Bunches and clusters

$$w \in B(v) \iff v \in C(w)$$

$$C(w) \leftarrow \{v \in V \mid \delta(w,v) < \delta(A_{i+1},v)\} \quad , \quad \text{if } w \in A_i - A_{i+1}$$

$$B(v) \leftarrow \bigcup_i \{w \in A_i - A_{i+1} \mid \delta(w,v) < \delta(A_{i+1},v)\}$$

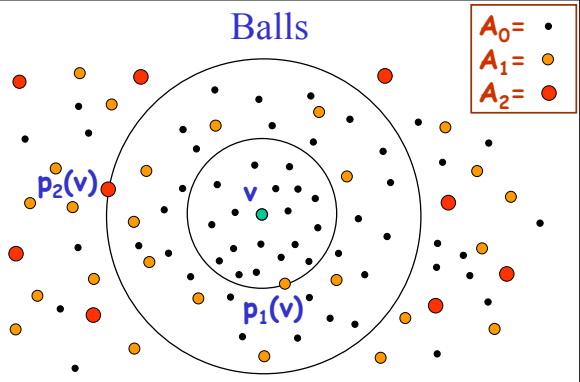
Part II

Spanners with sublinear surplus

The construction used above, when applied to unweighted graphs, produces spanners with sublinear surplus!

We present a slightly modified construction with a slightly simpler analysis.

Balls



$$Ball(u) = \{v \in V \mid \delta(u,v) < \delta(u, A_{i+1})\} \quad , \quad u \in A_i - A_{i+1}$$
$$Ball[u] = Ball(u) \cup \{p_{i+1}(u)\} \quad , \quad u \in A_i - A_{i+1}$$

The original construction

Select a hierarchy of centers $A_0 \supset A_1 \supset \ldots \supset A_{k-1}$.

For every $u \in V$, add to the spanner a shortest paths tree of $Clust(u)$.

The modified construction

Select a hierarchy of centers $A_0 \supset A_1 \supset \ldots \supset A_{k-1}$.

For every $u \in V$, add to the spanner a shortest paths tree of $Ball(u)$.

Spanners with sublinear surplus

Select a hierarchy of centers $A_0 \supset A_1 \supset \ldots \supset A_{k-1}$.

For every $u \in V$, add to the spanner a shortest paths tree of $Ball(u)$.

The path-finding strategy

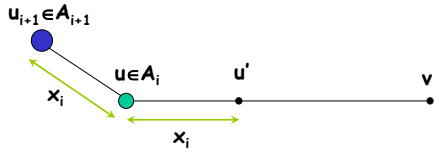
Suppose we are at $u \in A_i$ and want to go to v.

Let Δ be an integer parameter.

If the first $x_i=\Delta^i-\Delta^{i-1}$ edges of a shortest path from u to v are in the spanner, then use them.

Otherwise, head for the $(i+1)$-center u_{i+1} nearest to u.

► The distance to u_{i+1} is at most x_i. (As $u' \notin \text{Ball}(u)$.)

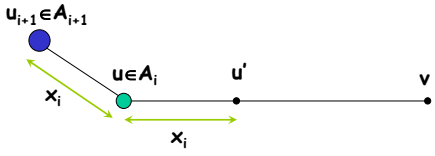


The path-finding strategy

We either reach v, or at least make $x_i=\Delta^i-\Delta^{i-1}$ steps in the right direction.

Or, make at most $x_i=\Delta^i-\Delta^{i-1}$ steps, possibly in a wrong direction, but reach a center of level $i+1$.

If $i=k-1$, we will be able to reach v.

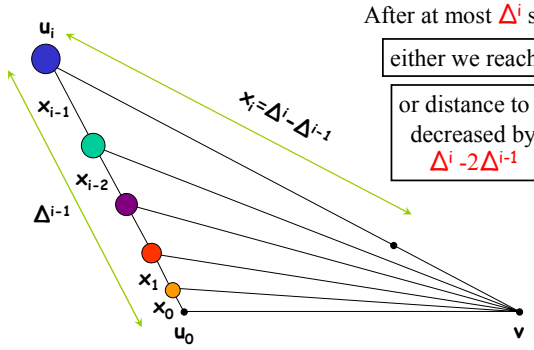


The path-finding strategy

After at most Δ^i steps:

either we reach v

or distance to v decreased by $\Delta^i - 2\Delta^{i-1}$



The path-finding strategy

After at most Δ^i steps:

either we reach v ➡ Surplus $2\Delta^{i-1}$

or distance to v decreased by $\Delta^i - 2\Delta^{i-1}$ ➡ Stretch $\frac{\Delta^i}{\Delta^i - 2\Delta^{i-1}} = 1+\frac{2}{\Delta-2}$

The surplus is incurred only once!

$$\delta'(u,v) \le (1+\frac{2}{\Delta-2})\cdot\delta(u,v) + 2\Delta^{k-2}$$

Sublinear surplus

$$\delta'(u,v) \le (1+\frac{2}{\Delta-2})\cdot\delta(u,v) + 2\Delta^{k-2}$$

$$\delta(u,v)=d \quad , \quad \Delta=\lceil d^{1/(k-1)}+2 \rceil$$

$$\delta'(u,v) \le d + O(d^{1-\frac{1}{k-1}})$$

Open problems

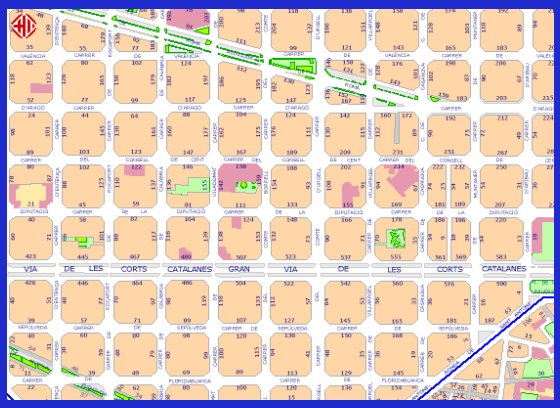
Arbitrarily sparse additive spanners?

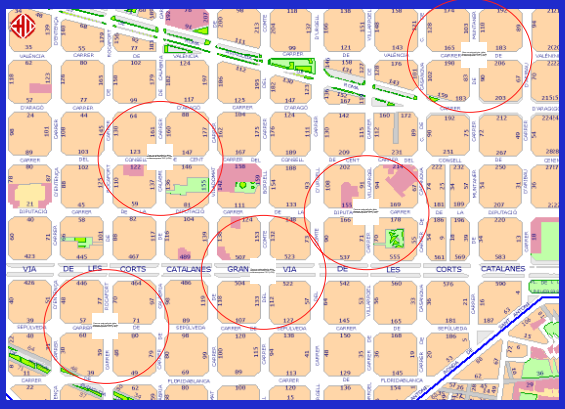
Distance oracles with sublinear surplus?

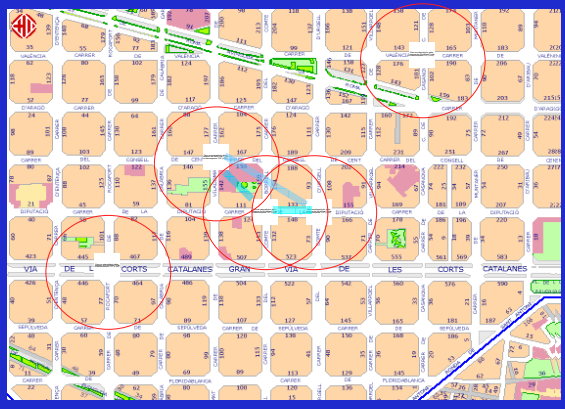
The walkers problem

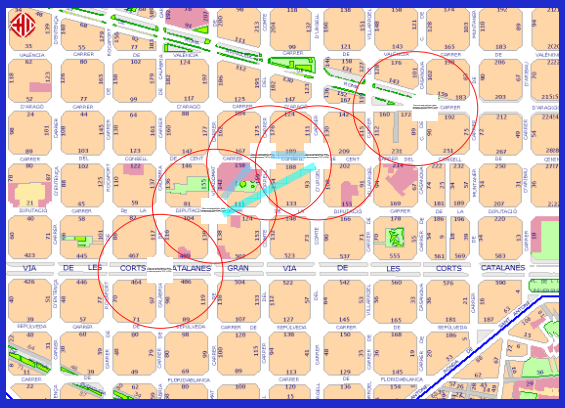
J.D., X.Perez, M.Serna, N.Wormald

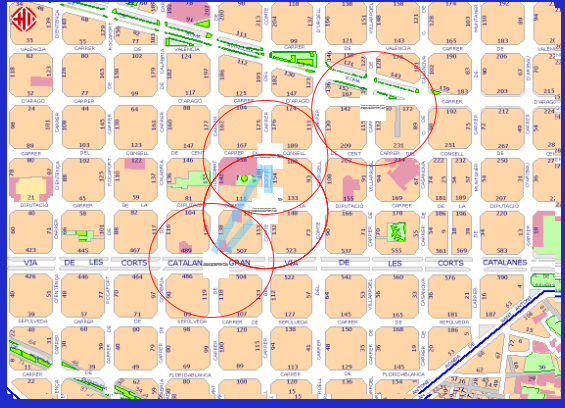
Partially supported by the EC 6th FP 001907: DELIS











GOAL

STUDY THE CONNECTIVITY OF THE AD-HOC NETWORK STABLISHED BETWEEN THE AGENTS, AS THESE MOVE FOLLOWING THE EDGES OF A GRAPH:

- Cycle
- Grid
- Hypercube
- Random Geometric graph

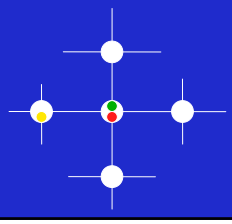
GOAL

STUDY THE ITERACTIONS OF SIMULTANEOUS RANDOM WALKS ON DIFFERENTS TOPOLOGIES.

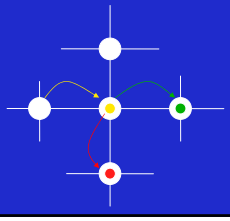
Walkers in the toroidal grid

- Given a set W ($|W|=w$) of walkers (agents, robots,..) which at each step, they can move N/S/E/W on the edges of a toroidal grid T_N, with $N=n^2$, the walkers have RF communication within a distance d (Manhatan, euclidian, etc.), we wish to study the evolution of the connectivity graph $G_t[W]$, as the walkers move.

- At step $t=0$, the w walkers are sprinkled u.a.r. on T_N. $f: W \rightarrow V(T_N)$ (static case)
- At each step t, every walker is forced to move

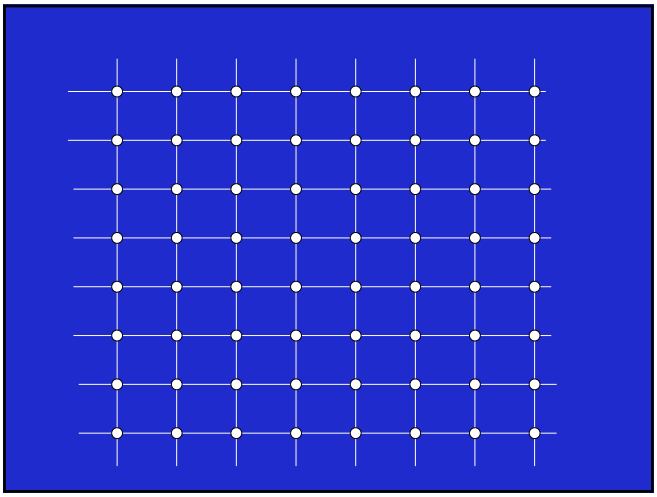


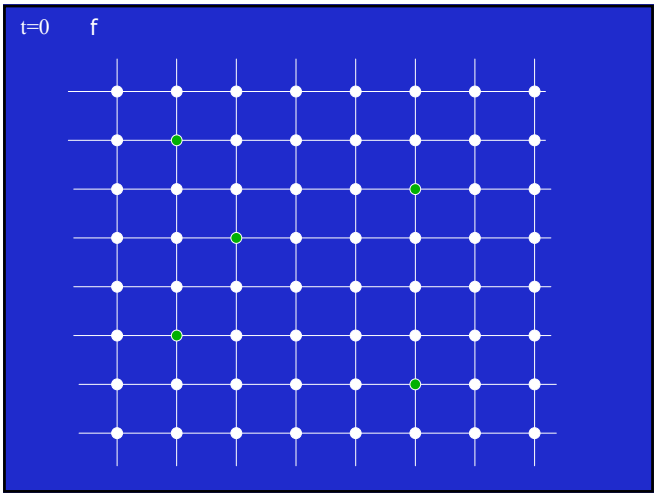
- At step $t+1$, every walker is forced to move

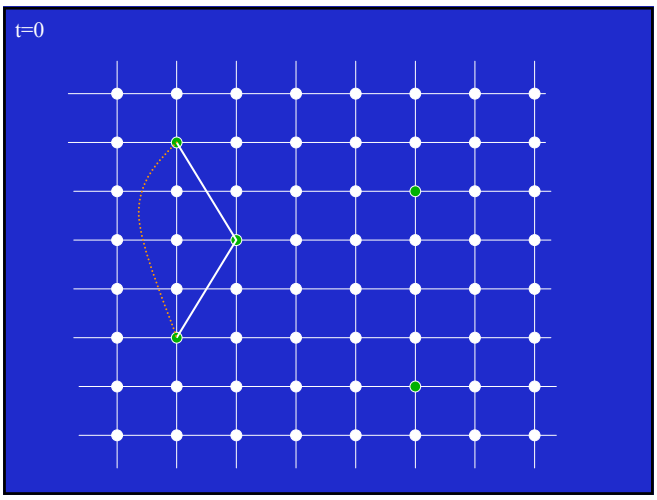


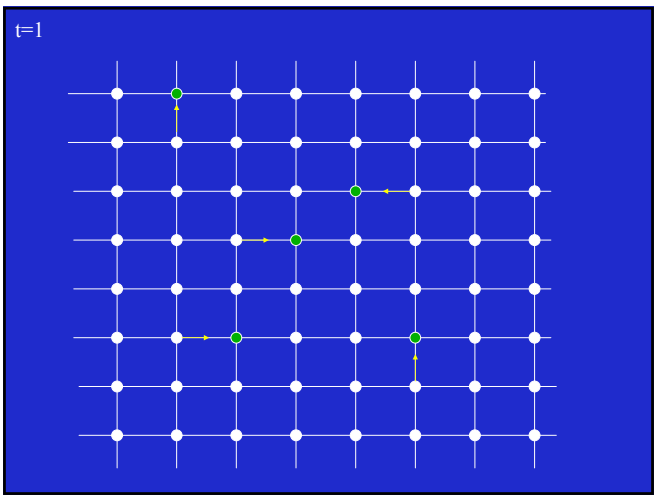
Toy example

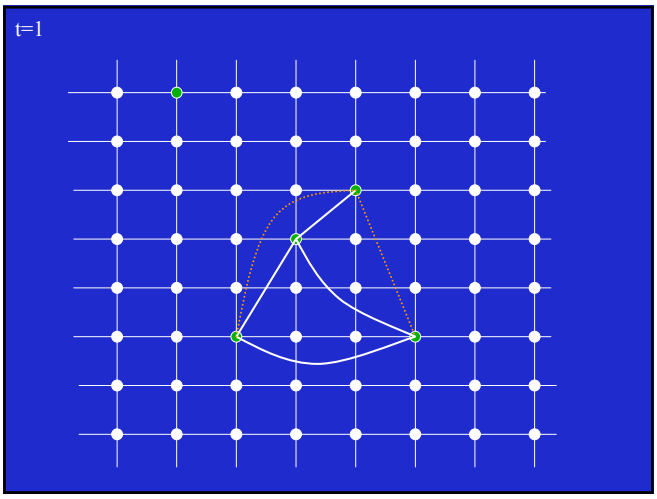
- At $t=0$, sprinkle 5 walkers in a nxn grid, with a max communication distance $d=3$ (in the l^2 norm)
- Look evolution of $G_t[W]$ up to $t=4$.

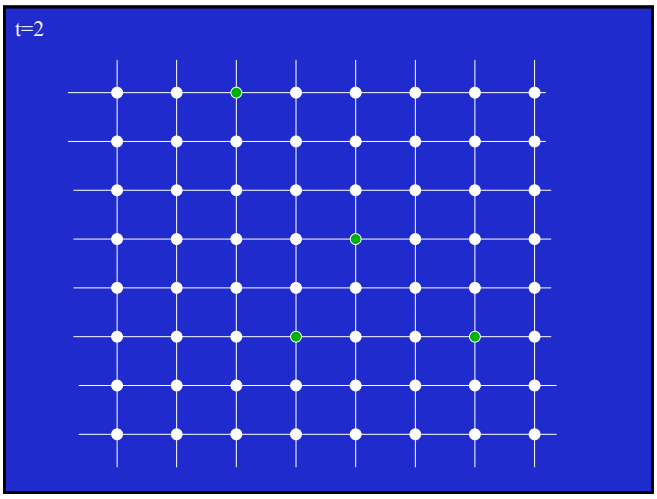


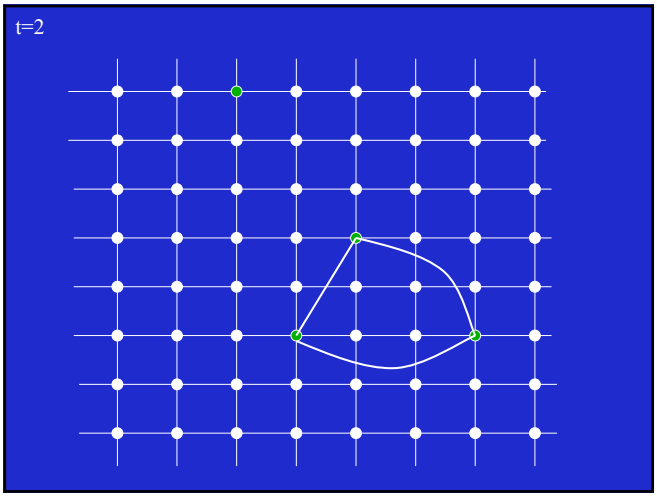

t=0
f

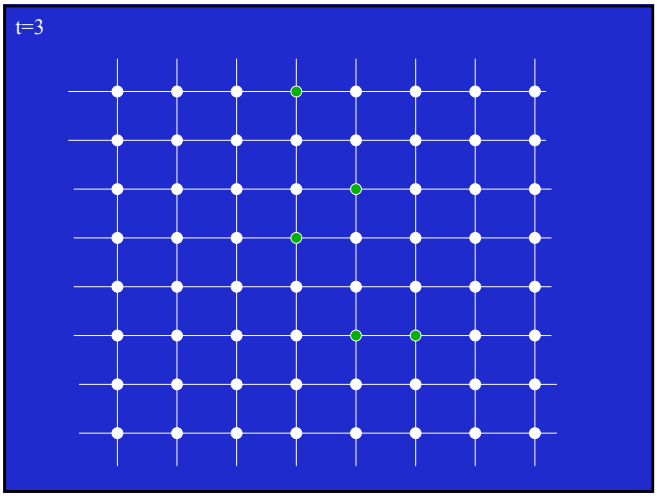

t=0

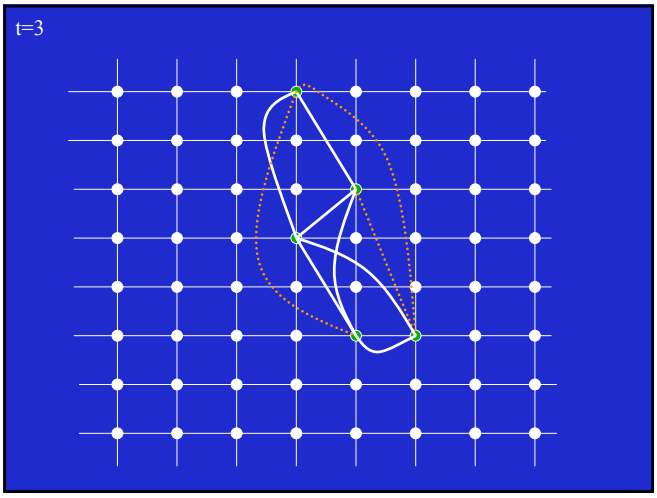

t=1

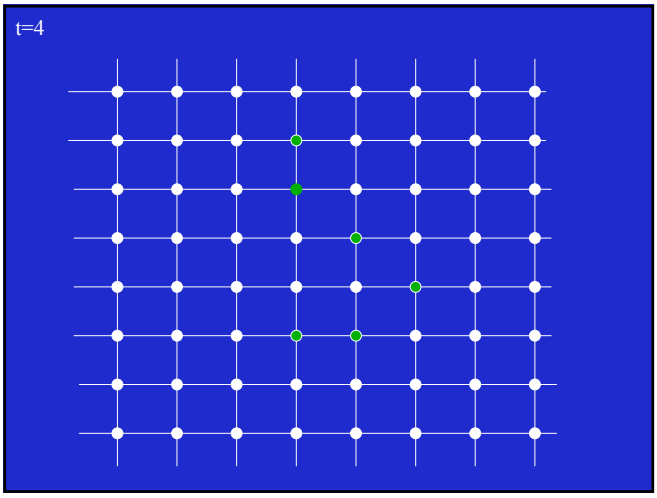

t=1

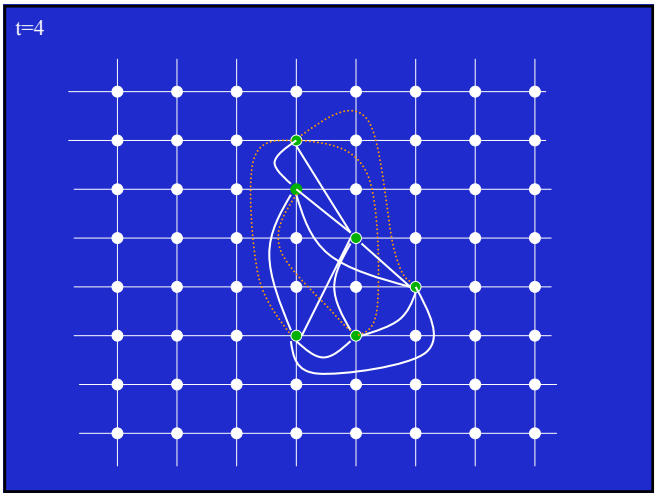

t=2









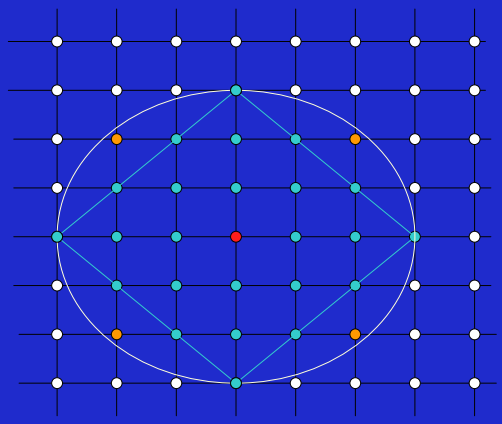


Static case

Some parameters

- K = # connected components in $G_f[W]$
  $\rho = w/N$ (expected walkers per node)
- h = minimum number vertices around a simple component.
- Simple component: isolated vertex in $G_f[W]$

h for l^1 and l^2 distances (for $d=3$)



Some values for h

l^1 $h=2d(d+1)$

l^2 $h \sim \pi d^2$ for large d

l^∞ $h=4d(d+1)$

Observation

- If $d \geq 2n$ → $G_f[W]$ is connected
- If $d^2 = \Omega(N/\sqrt{w})$ → $G_f[W]$ connected a.a.s. →
- Interesting case of study: $d^2 = o(N/\sqrt{w})$ $d = o(n)$

Random variables

- X = number simple components
- K = number connected components

Let $\mu = N(1-e^{-\rho})\, e^{-h\rho}$. Then

$\mu \sim w\ e^{-h\rho}$ if $\rho = w/N \to 0$,

$\mu \sim N(1-e^{-\rho})\, e^{-h\rho}$ if $\rho = w/N \to c$,

$\mu \sim N e^{-h\rho}$ if $\rho = w/N \to \infty$.

Shape distribution of X

Theorem The expected number of simple Components satisfy $E[X]= N(1-e^{-\rho})(1-h/N)^w$ Moreover

- If $\mu \to 0$ *then* $E[X] \to 0$, there are no simple components a.a.s.
- If $\mu \to \infty$ there are simple components a.a.s.
- If $\mu=\Theta(1)$ then X is Poisson with mean μ

Corollary. The probability of not having simple Components is

$$Pr[X=0]=e^{-\mu}+o(1).$$

Sketch of proof

Compute the *K-th* moment:

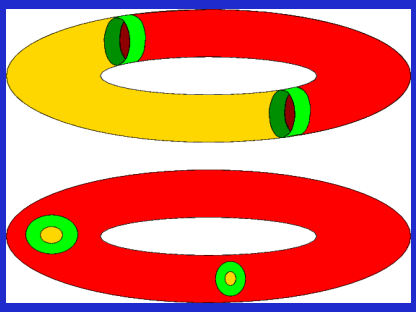
$\mu_k=E[[X]_k]=\Sigma\, Pr[S_{v1}=1 \wedge \ldots \wedge S_{vk}=1]$

where $S_{vi}=1$ if v_i is the center of a simple component, otherwise $S_{vi}=0$, and the sum is over all k-tuples of vertices which occupy different walkers.

Use inclusion-exclusion ..

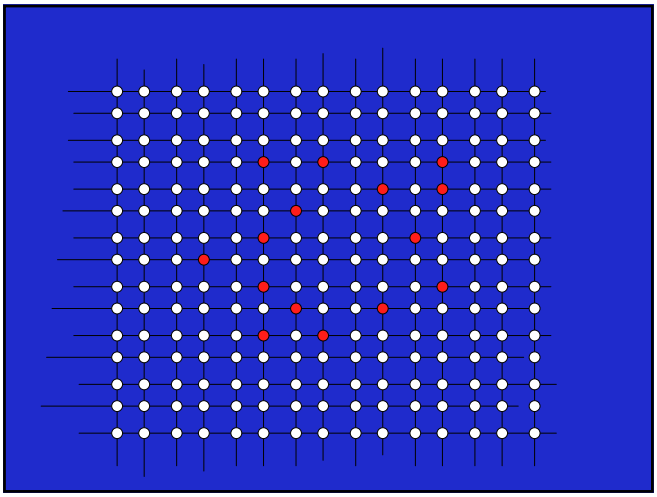
- A r-component a non-simple component which can be embedded in a $i \times j$ grid $(i,j<n)$
- A nr-component a non-simple component which is not r-component

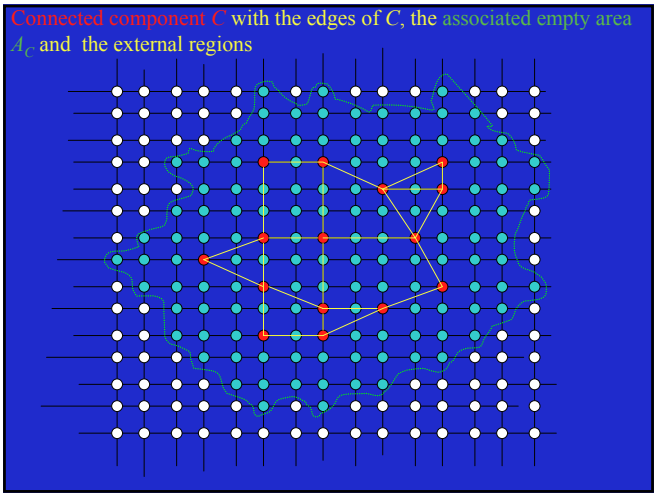
nr-components

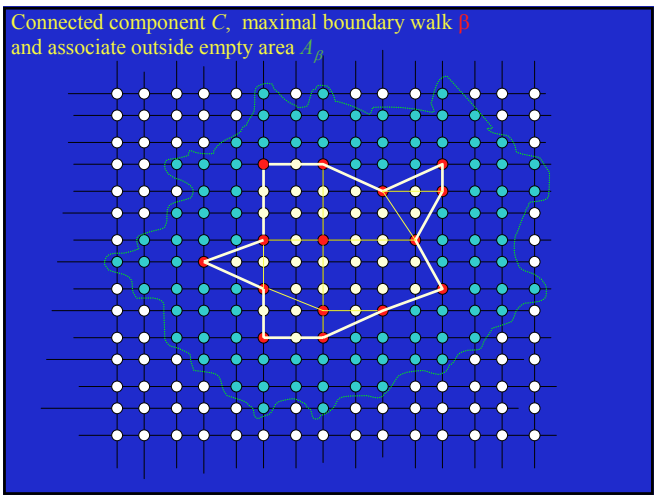


- X = # simple components
- Y = # r-components
- Z_1 = # nr-components which can not coexists with other nr-components
- Z_2 = # non type 1 nr-components

$$K= X+Y+Z_1+Z_2$$







Geometric Lemma

Let C be a component in T_N with β a max. boundary walk of length l. Then

$|A_\beta| > dl/10^{10}$

If C is rectangular, then $|A_\beta| > h+dl/10^{10}$

Simple components are predominant a.a.s. in T_N

Lemma

If $h\rho=hw/N\to\infty$, then

- $E[Y]=o(E[X])$
- $E[Z_2]=o(E[X])$

Connectivity of $G_\beta[W]$

Theorem

For $\mu\to\Theta(1)$, aas $G_\beta[W]$ consists of simple components and a giant connected component

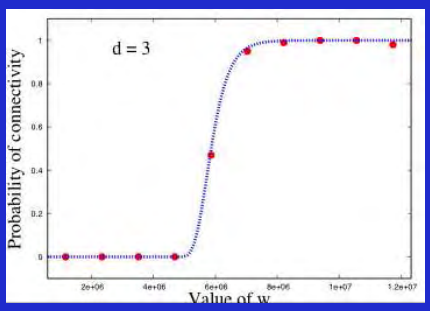
Corollary. If w walkers are placed uar on T_N, the probability that $G_\beta[W]$ is connected is $e^{-\mu}+o(1)$.

Threshold for connectivity
d vs w

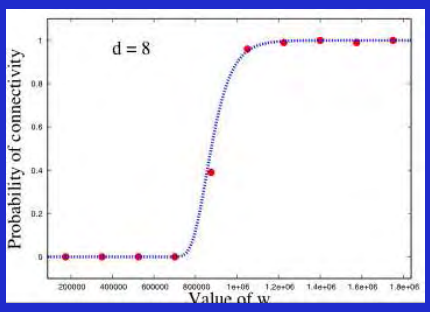
Corollary. If $\mu = \Theta(1)$:

- If $h = \Theta(1)$ iff $w = \Theta(N \log N)$
- If $h = \Theta(\log N)$ iff $w = \Theta(N)$
- If $h = \Theta(N^c \log N)$ iff $w = \Theta(N^{1-c})$
- If $h = \Theta(N/\log N)$ iff $w = \Theta(\log N \log\log N)$

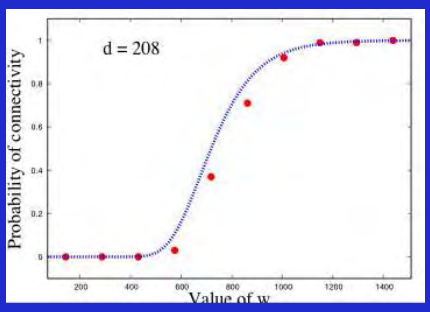
3000x3000; d=cte



3000x3000; d=log n w=875018

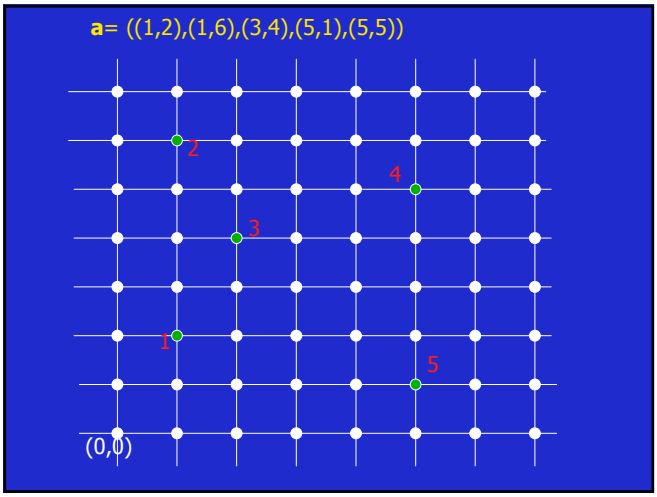


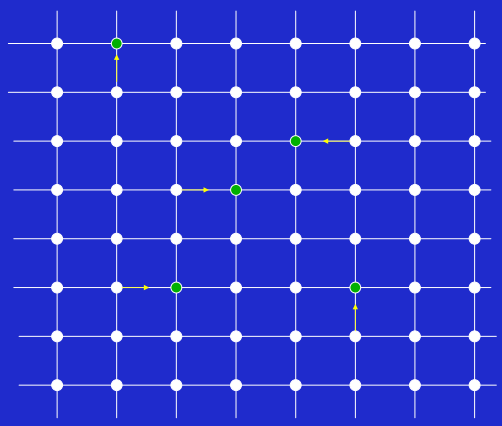
3000x3000; $n^{2/3}$ w=719



Dynamic properties

Consider labelled (x,y) all vertices in T_N
Given f of $\{1,\ldots,w\}$ on T_N, a configuration (as t evolves) is a vector $\boldsymbol{a}=(a_1,a_2,..,a_w)$, where $a_i=(a_{ix},a_{iy})$ is the label of vertex in which walker i is.





Let the graph M:
V(M)={configurations} and
(***a***, ***b***) in E(M) if $\exists i$ dist$(a_i,b_i)=1$

Notice: $\delta(\boldsymbol{a}) = 4^w$.
The dynamic process is a random walk on M.

Hitting time h_{ab} in M

If N is even, ***a*** and ***b*** have the same parity iff $\forall i,j$
$(a_{ix}-a_{jx})+(a_{iy}-a_{jy})=(b_{ix}-b_{jx})+(b_{iy}-b_{jy})$ mod 2.

Lemma Given ***a, b*** in M,
If N is odd, M is ergodic and h_{ab} is finite.
If N is even, M no es ergodic but if ***a*** and ***b*** have the same parity, h_{ab} is finite.

Therefore, the system always reaches a state representing a single connected component, within finite expected time

Notice The initial uniform distribution stays invariant as t evolves.

So we need to consider only the case $\mu=\Theta(1)$.

(if $\mu \to 0$ then Gt[W] aas connected
if $\mu \to \infty$ then Gt[W] aas disconnected)

Dynamic random variables

- $X(t)$ = number simple components at time t
- $S(t)$ = number simple components surviving between t and $t+1$
- $B(t)$ = number simple components born between t and $t+1$
- $D(t)$ = number simple components dying between t and $t+1$

Theorem. *S(t), B(t), D(t)* are asymptotically jointly independent Poisson and

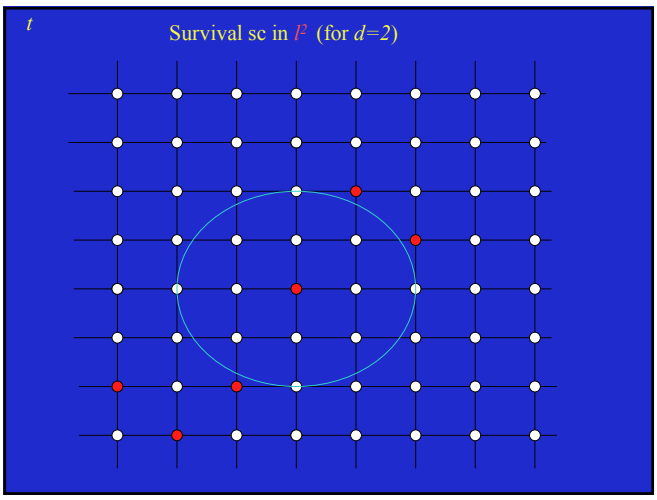
$E[S(t)] \sim \mu$	if $dw/N \to 0$,
$E[S(t)] \sim \mu - \lambda$	if $dw/N \to c$,
$E[S(t)] \sim 4\mu(1-e^{-\rho/4})/(1-e^{-\rho})$	if $dw/N \to \infty$,
$E[B(t)] = E[D(t)] \sim d\mu\rho$	if $dw/N \to 0$,
$E[B(t)] = E[D(t)] \sim \lambda$	if $dw/N \to c$,
$E[B(t)] = E[D(t)] \sim \mu$	if $dw/N \to \infty$,

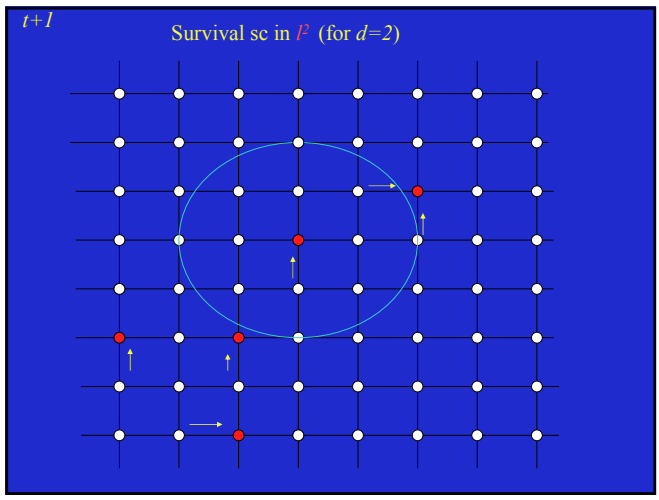
with $\lambda=(1- e^{-d\rho})\mu$.

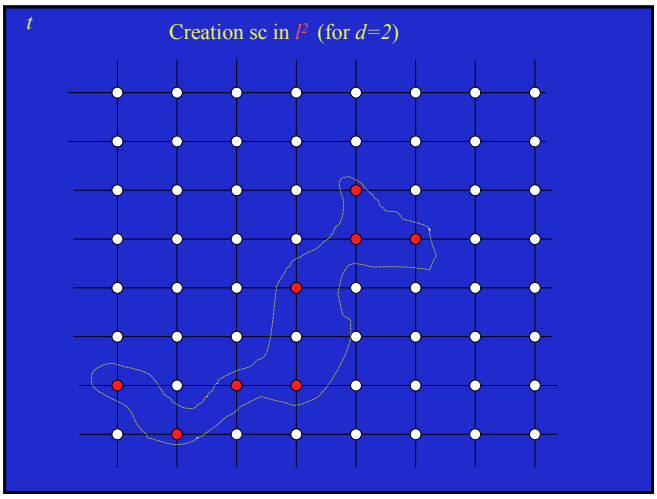
Sketch of proof: consider all cases of S, B, D

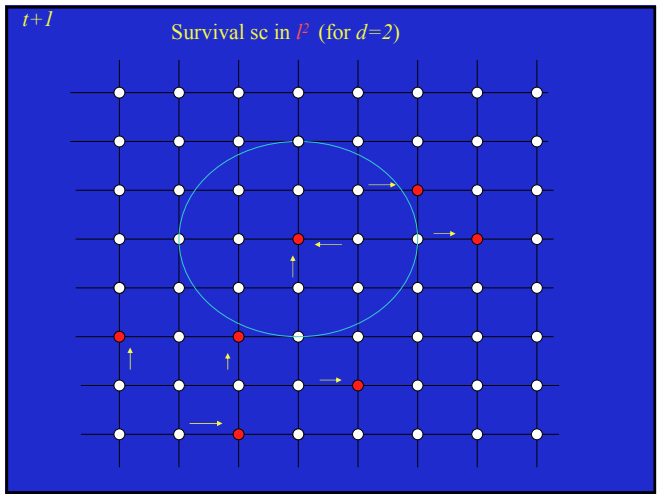
Show that S, B, B are jointly asymptotic Poisson

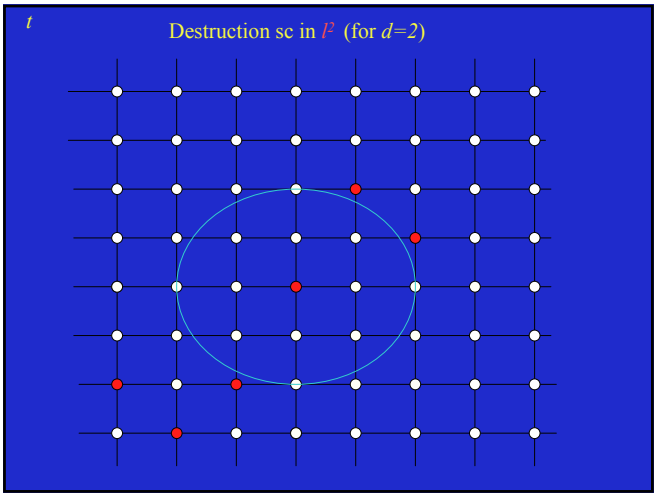
$$E[[S]_q.[B]_r.[D]_p] = \mu_1^q.\mu_1^r.\mu_1^p$$

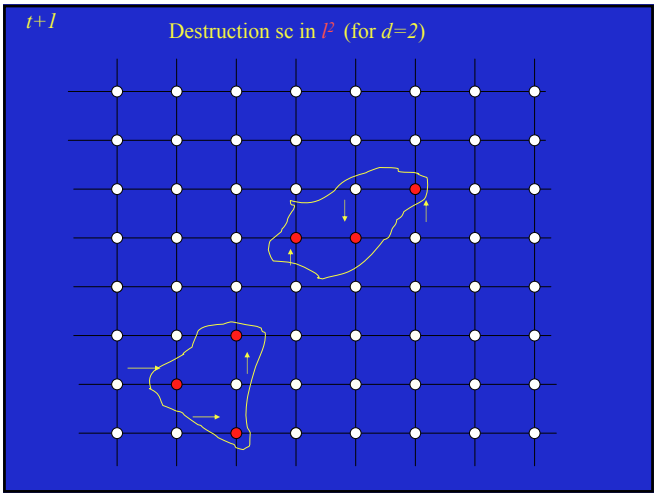












Prob $G_t[W]$ connected and $G_{t+1}[W]$ disconnected

Theorem.

$Pr[X(t+1)\geq 1 \text{ and } X(t)=0] \sim$

$\mu e^{-\mu} b\rho$ if $d\rho \to 0$,

$e^{-\mu}(1-e^{-\lambda})$ if $d\rho \to c$,

$e^{-\mu}(1-e^{-\mu})$ if $d\rho \to \infty$.

Average lifespan of simple component

Lifespan of simple component: number of steps from creation to destruction.

L_{vt}: lifespan simple component at v, between t and t+1.

Average lifespan L_T of simple components born in [0,T-1]

$$L_T = (\sum_t \sum_v L_{vt}) / |\{(v,t) : L_{vt} > 0\}|$$

Average lifespan of simple component

Theorem

$L \sim 1/d\rho$ if $d\rho \to 0$

$L \sim \mu/\lambda$ if $d\rho \to c$

$L \sim 1$ if $d\rho \to \infty$

Average connectiveness

Let C be the average connectivity of $G_t[W]$

The random variable counting the expected length of any connected period

Theorem

$C \sim 1/d\rho\mu$ if $d\rho \to 0$

$C \sim 1/(1-e^{-\lambda})$ if $d\rho \to c$

$C \sim 1/(1-e^{-\mu})$ if $d\rho \to \infty$

Average disconnectiveness

Let D be the average disconnectivity of $G_t[W]$

Theorem

$D \sim (e^{-\mu} - 1)/d\rho\mu$ if $d\rho \to 0$

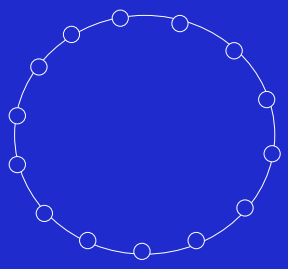
$D \sim (e^{-\mu} - 1)/(1 - e^{-\lambda})$ if $d\rho \to c$

$D \sim e^{-\mu}$ if $d\rho \to \infty$

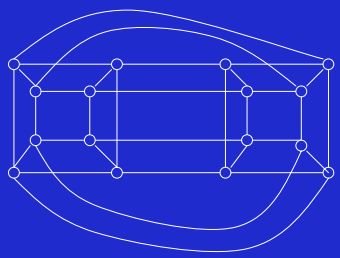
$N = 1000 \times 1000$		Experimental average	Modified prediction
$d = 3$	Time $G_{f_t}[W]$ stays connected	1.93	2.08
$w = 555377$	Time $G_{f_t}[W]$ stays disconnected	2.14	2.02
$d = 7$	Time $G_{f_t}[W]$ stays connected	2.05	2.01
$w = 106128$	Time $G_{f_t}[W]$ stays disconnected	2.70	2.88
$d = 10$	Time $G_{f_t}[W]$ stays connected	2.28	2.20
$w = 50804$	Time $G_{f_t}[W]$ stays disconnected	3.17	2.49
$d = 32$	Time $G_{f_t}[W]$ stays connected	4.89	4.97
$w = 4113$	Time $G_{f_t}[W]$ stays disconnected	7.56	8.15
$d = 100$	Time $G_{f_t}[W]$ stays connected	14.14	15.26
$w = 301$	Time $G_{f_t}[W]$ stays disconnected	27.86	33.42
$d = 145$	Time $G_{f_t}[W]$ stays connected	18.97	21.35
$w = 122$	Time $G_{f_t}[W]$ stays disconnected	55.20	63.51

Similar results obtained for:

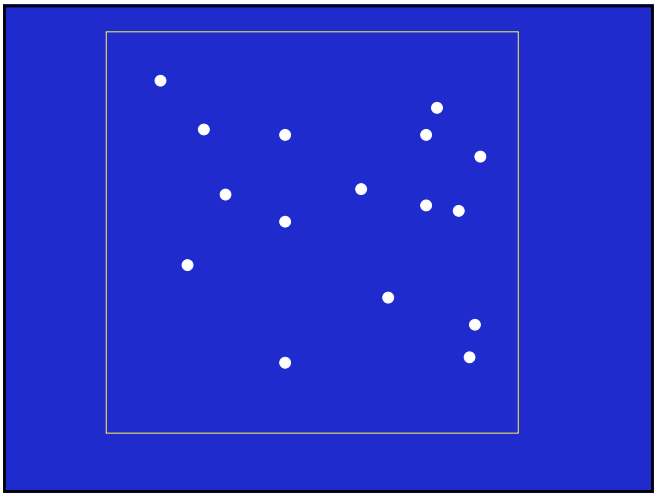
Cycle C_N

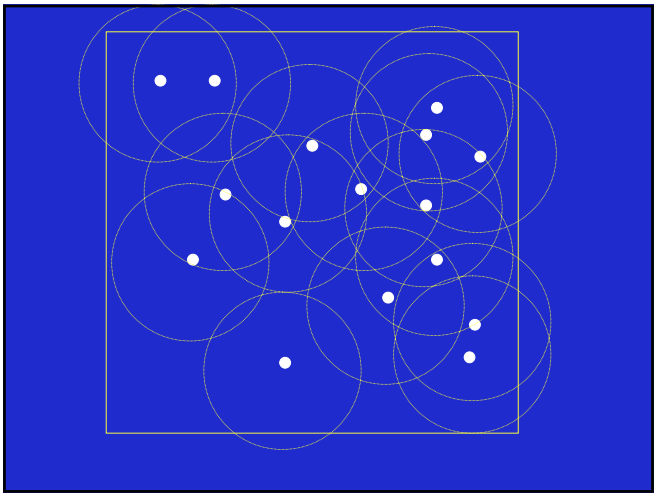


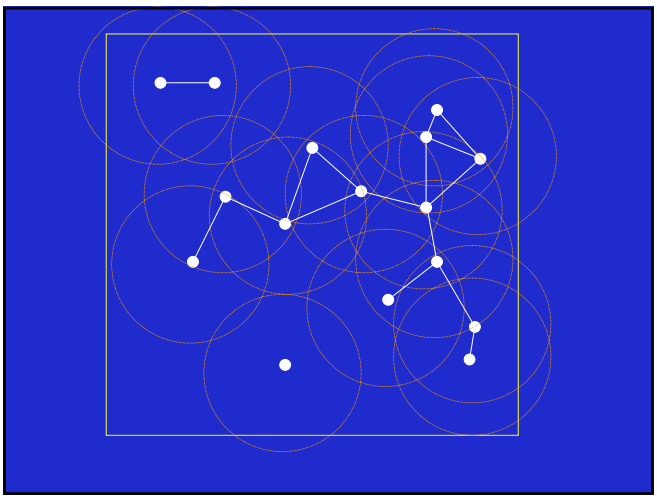
n-dimensional hypercube: H_N

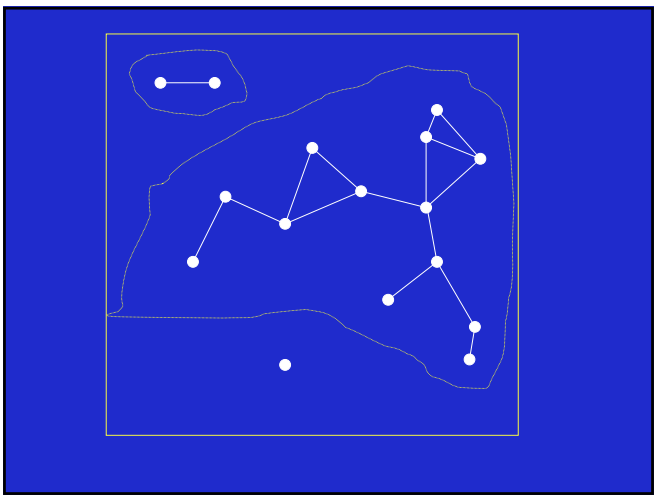


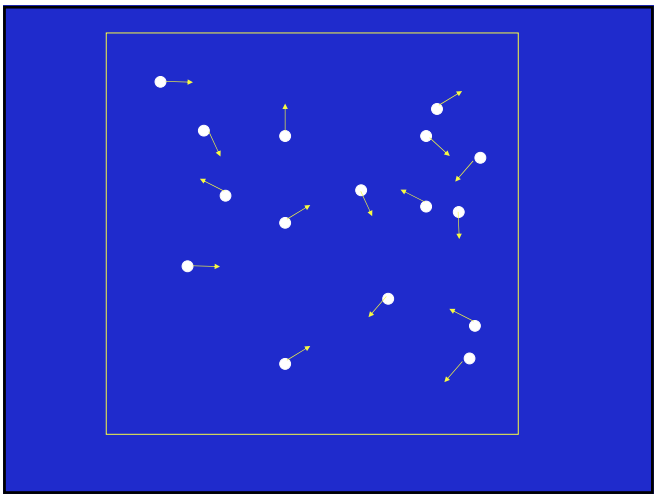
Future work on Random Geometric Graphs

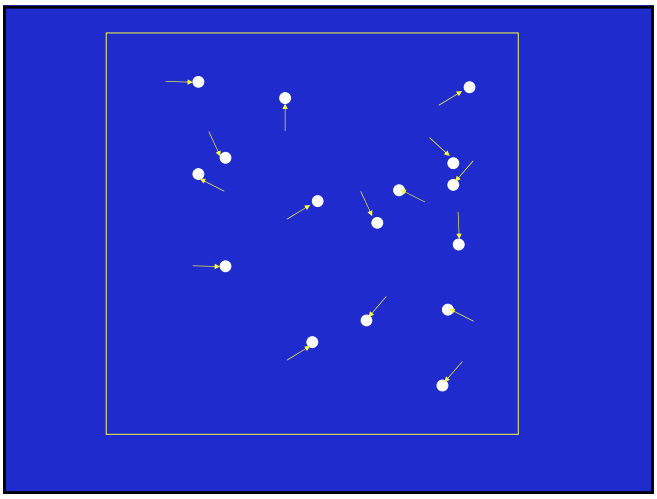


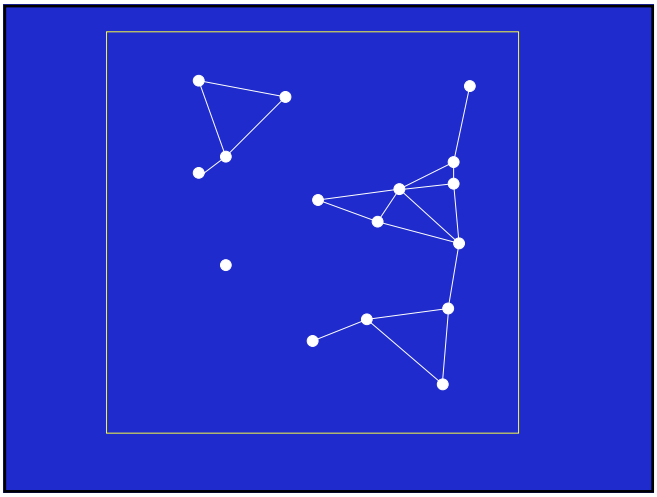










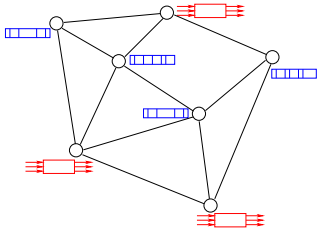


ありがとう

Approximation Algorithms for Network Problems

Susanne Albers
University of Freiburg
Germany

Large networks

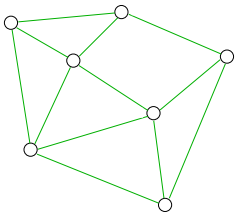


Buffer management in switches
Online, competitive analysis
A., Schmidt STOC'04

Web caching, request reordering
Offline, approx. algorithms
A. SPAA'04

Network creation game
Nash equilibria, price of anarchy
A. 05

Large networks

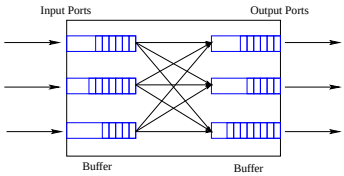


Buffer management in switches
Online, competitive analysis
A., Schmidt STOC'04

Web caching, request reordering
Offline, approx. algorithms
A. SPAA'04

Network creation game
Nash equilibria, price of anarchy
A. 05

Buffer management in switches

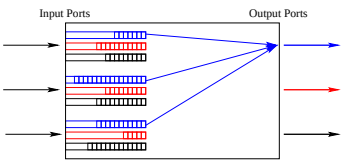


Switches forward data packets.

Buffers store packets temporarily if capacity available.

Goal: maximize throughput.

Virtual output queueing



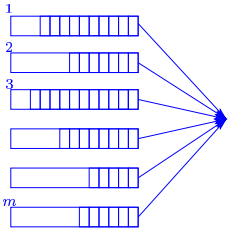
Each input port i maintains for each output port j a queue Q_{ij}.

Problem

m buffers, each of which can store B packets.

In each time step
– new packets arrive online
P_i: #packets in buffer i
N_i: #new packets at buffer i
paket loss: $\max\{N_i + P_i - B, 0\}$
– one buffer can send one paket to the output

Goal: maximize #transferred pakets



Competitive analysis

Online problem

A: Online algorithm	OPT: Offline algorithm
$A(\sigma)$	$OPT(\sigma)$

A is c-competitive if $\exists a$ such that for all sequences σ

$$A(\sigma) \geq \frac{1}{c} \cdot OPT(\sigma) - a.$$

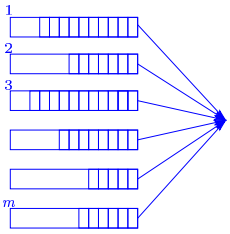
Previous results

- Every reasonable algorithm is 2-competitive.
- Randomized upper bound: $e/(e-1) \approx 1.58$
  Azar, Richter 2003
- Lower bounds
  Deterministic: 1.366
  Randomized: 1.46 ($B = 1$)
  Azar, Richter 2003
- Single buffer problems: pakets have values
  Upper bounds: 2, 1.75
  Kesselman et al. 2001; Bansal et al. 2004

Greedy algorithms

Greedy: Always serve a buffer currently storing a maximum number of packets.

Advantages:
– fast
– little extra memory
– best strategy to avoid packet loss



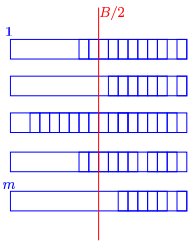
Our results

- Exact performance of all Greedy algorithms: 2-competitive
- New algorithm Semi-Greedy: $17/9 \approx 1.89$
  fast, little extra memory, serves full buffers
- Lower bounds (B arbitrary)
  Deterministic: $e/(e-1) \approx 1.58$
  Randomized: 1.46
- Extra resources: larger buffers, higher transmission rates
  Almost matching upper and lower bounds
- Optimal offline algorithm running in polynomial time

Semi-Greedy

In each time step execute the first applicable rule.

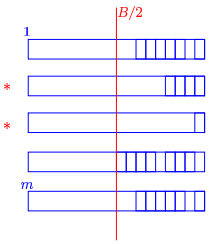
1. $\exists$ buffer with $> B/2$ packets
   $\rightarrow$ serve a buffer with max. number of packets
2. $\exists$ non-empty buffer that has never been full
   $\rightarrow$ amongst these, serve one with max. number of packets
3. Serve a buffer with max. number of packets



Semi-Greedy

In each time step execute the first applicable rule.

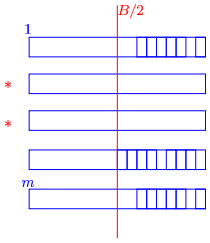
1. $\exists$ buffer with $> B/2$ packets
   $\rightarrow$ serve a buffer with max. number of packets
2. $\exists$ non-empty buffer that has never been full
   $\rightarrow$ amongst these, serve one with max. number of packets
3. Serve a buffer with max. number of packets



Semi-Greedy

In each time step execute the first applicable rule.

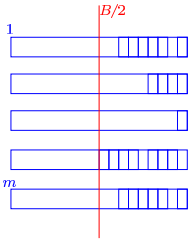
1. $\exists$ buffer with $> B/2$ packets
   $\rightarrow$ serve a buffer with max. number of packets
2. $\exists$ non-empty buffer that has never been full
   $\rightarrow$ amongst these, serve one with max. number of packets
3. Serve a buffer with max. number of packets



Semi-Greedy

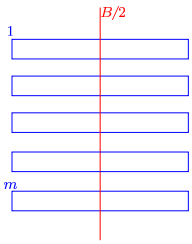
In each time step execute the first applicable rule.

1. $\exists$ buffer with $> B/2$ packets
   $\rightarrow$ serve a buffer with max. number of packets
2. $\exists$ non-empty buffer that has never been full
   $\rightarrow$ amongst these, serve one with max. number of packets
3. Serve a buffer with max. number of packets



Semi-Greedy

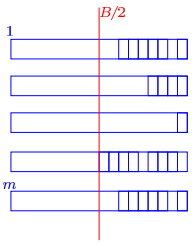
Whenever all buffers are empty, the hitherto maximum load of each queue is set to 0.



Semi-Greedy

In each time step execute the first applicable rule.

1. $\exists$ buffer with $> B/2$ packets
   $\rightarrow$ serve a buffer with max. number of packets
2. $\exists$ non-empty buffer that has never been full
   $\rightarrow$ amongst these, serve one with max. number of packets
3. Serve a buffer with max. number of packets

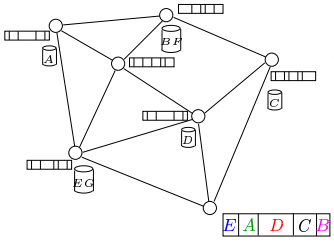


Analysis

Partition input into subsequences so that at the end of each subsequence Semi-Greedy's buffers are empty.

Compare: throughput Semi-Greedy / throughput OPT

Web caching



Documents are text files, images, html pages, ...

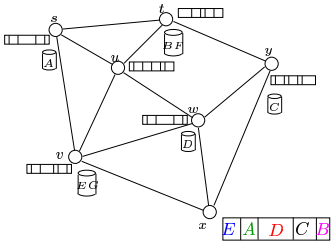
Important properties:
documents have different sizes and incur different costs

Web caching

Request: (x, D) x requests documents D

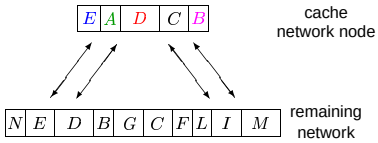
D not in x's cache: Cost(D)
Optional: loading D

Goal: Minimize total service cost



$\sigma = (x, D)\,(y, E)\,(z, A)\,(v, C)\,(w, B)\,(x, F)\ldots$

Web caching

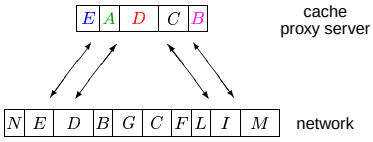


$\sigma = D\ C\ A\ B\ C\ F\ E\ C\ N\ I\ L\ M\ B\ E\ A\ L\ I\ F$

Goal: Serve a sequence of requests
so that the total service cost at the node is minimized.

Request reordering

Proxy server: requests are independent



$\sigma = D\ C\ A\ B\ C\ F\ E\ E\ A\ N\ L\ M\ B\ E\ A\ L\ I\ F$
(r)

$\sigma(j)$ may be served before $\sigma(i)$ if $j - i < r$ $\quad r \in \mathbf{N}$

Advantage: improved cache hit rates

Feder, Motwani, Panigrahy, Zhu 2002

Cost models

Document D Size(D) Cost(D)

Uniform Model:
Cost(D) = Size(D) = 1

Bit Model:
Cost(D) = Size(D)

Fault Model:
Cost(D) = 1

General Model:
Cost(D) arbitrary

Previous results, reordering

Online
Uniform Model: $(K/s+2)$-competitive (deterministic)
Bit and Fault Models: $(K/s+3)$-competitive (deterministic)

Offline
General Model: Polynomial algorithm for cache size 1 if
r logarithmic in $|\sigma|$ or #distinct documents is constant

K = size cache s = size smallest document

Feder, Motwani, Panigrahy, Seiden, van Stee, Zhu 2003

Our results

Online
General Model: optimal $(K/s+1)$-competitive alg. (deterministic)

Offline

	Approximation	Extra memory	$S = \max$ Size
Uniform Model:	2	–	
Bit Model:	$2+\epsilon$	$\frac{1}{(1+\epsilon/2)}S$	$\epsilon \geq 0$
Fault Model:	$2+\epsilon$	$(1+2/\epsilon)S$	
General Model:	8	–	

Approach: reduce problem to one of computing batched schedules.

Batched processing

$\sigma = \underbrace{\sigma(1) \ldots \sigma(r)}_{B_1}\ \sigma(r+1) \ldots \sigma(2r)\ \sigma(2r+1) \ldots \sigma(3r)\ldots$

Batch i

$B_i = \sigma(ir+1)\ldots\sigma(ir+r)$

Batched processing

$\sigma = \sigma(1) \ldots \sigma(r)\ \underbrace{\sigma(r+1) \ldots \sigma(2r)}_{B_2}\ \sigma(2r+1) \ldots \sigma(3r)\ldots$

Batch i

$B_i = \sigma(ir+1)\ldots\sigma(ir+r)$

Batched processing

$\sigma = \sigma(1) \ldots \sigma(r)\ \sigma(r+1) \ldots \sigma(2r)\ \underbrace{\sigma(2r+1) \ldots \sigma(3r)}_{B_3}\ldots$

Batch i

$B_i = \sigma(ir+1)\ldots\sigma(ir+r)$

Batched processing

Lemma: Suppose that A serves σ with cost C.
Then there exists A' that processes σ in batches and incurs a cost of at most $2C$.

Uniform Model

$\sigma = \ldots\ldots \underbrace{\sigma(ir+1) \ldots \sigma(ir+r)}_{B_i} \ldots\ldots$

Algorithm BMIN

1. Serve requests to documents in cache;
2. **while** $\exists D \in B_i$ with unserved requests **do**
   Serve requests to D;
   Determine E in cache whose next unserved request is farthest in future;
   if next unserved request to E is in a later batch than that to D **then**
   Load D by evicting E;

Uniform Model

Algorithm BMIN

1. Serve requests to documents in cache;
2. **while** $\exists D \in B_i$ with unserved requests **do**
   Serve requests to D;
   Determine E in cache whose next unserved request is farthest in future;
   if next unserved request to E is in a later batch than that to D **then**
   Load D by evicting E;

$\sigma = \ldots\ldots \underbrace{A\ B\ A\ A\ D}_{B_i} \ldots\ldots \underbrace{A\ B\ B\ D\ D}_{B_j} \ldots\ldots \underbrace{B\ A\ B\ B\ E}_{B_k}$

A
B
E

Uniform Model

Algorithm BMIN

1. Serve requests to documents in cache;
2. **while** $\exists D \in B_i$ with unserved requests **do**
   Serve requests to D;
   Determine E in cache whose next unserved request is farthest in future;
   if next unserved request to E is in a later batch than that to D **then**
   Load D by evicting E;

$$\sigma = \ldots\ldots \underbrace{A\ B\ A\ A\ D}_{B_i} \ldots\ldots \underbrace{A\ B\ B\ D\ E}_{B_j} \ldots\ldots \underbrace{B\ A\ B\ B\ E}_{B_k}$$

A
B
E

Uniform Model

Lemma: BMIN is optimal among algorithms processing request sequences in batches.

Theorem: BMIN achieves an approximation ratio of 2.

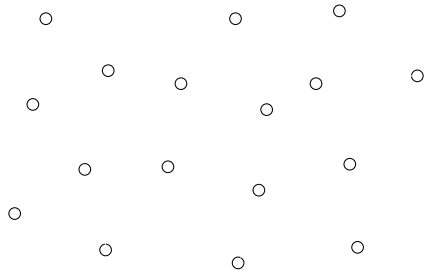
Approximations

Construct schedules that serve σ in batches

Bit, Fault Models: Formulate problems as ILP.

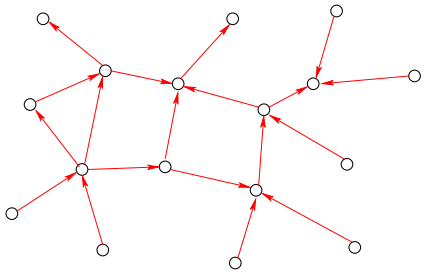
General Model: Formulate problem as a loss minimization problem.
Bar-Noy, Bar-Yehuda, Freund, Naor, Schieber 2001

Network creation game



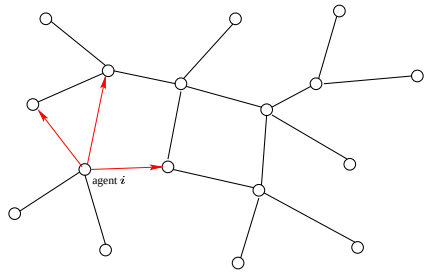
n agents have to build a connected network.
Fabrikant, Lutha, Maneva, Papadimitriou, Shenker PODC'03

Network creation game



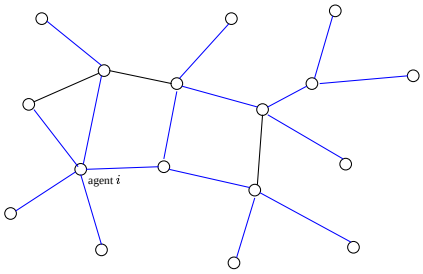
n agents have to build a connected network.
Fabrikant, Lutha, Maneva, Papadimitriou, Shenker PODC'03

Network creation game



Cost of $\alpha \geq 0$ for each edge.
Fabrikant, Lutha, Maneva, Papadimitriou, Shenker PODC'03

Network creation game



Shortest path distance to agent j, for all $j \neq i$.
Fabrikant, Lutha, Maneva, Papadimitriou, Shenker PODC'03

Problem

n agents $\quad \alpha \geq 0$

Cost(agent i) $=$ α #edges built by agent i

$+ \sum_{j \neq i}$ shortest path distance to agent j

Nash equilibria

No agent can improve its cost if other agents keep their strategies.

Price of anarchy:

$$P = \max_{\text{Nash eq.}} \frac{\sum_i \text{Cost(agent } i)}{\text{Cost(OPT)}}$$

Koutsoupias, Papadimitriou '99

Previous results

Fabrikant, Lutha, Maneva, Papadimitriou, Shenker PODC'03

$\alpha \leq 1, \quad \alpha > n^2$
P is constant

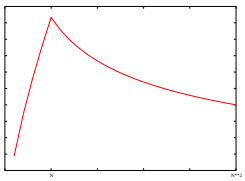
$1 < \alpha \leq n^2$
P is bounded by $\sqrt{\alpha}$

Tree-conjecture: $\exists\, C$ s.t. for $\alpha > C$ every Nash equilibrium is a tree.

Our results

$\alpha > 0$: $\quad P = O(1 + (\min\{\frac{\alpha^2}{n}, \frac{n^2}{\alpha}\})^{1/3})$

$\alpha \leq \sqrt{n}$: $\quad P$ is constant
$\sqrt{n} < \alpha \leq n$: $\quad P$ increasing, bounded by $n^{1/3}$
$n < \alpha$: $\quad P$ decreasing, constant for $\alpha \geq n^2$



Our results

Upper bounds can be extended to:
Weighted game: t_{ij} = traffic sent from agent i to j
Cost sharing: agent can pay for a fraction of an edge

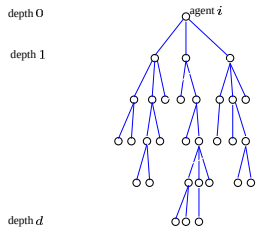
For any n and $n/4 \leq \alpha \leq n/3$
$\exists$ Nash equilibria that contain cycles.
Transient: $\exists$ seq. of players' changes leading to non-equilibrium state.

Nash equilibrium representing a chordal graph is transient.

Upper bound

Nash equilibrium N $G = (V, E)$

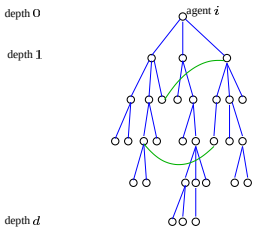
Shortest path tree rooted at agent i



Upper bound

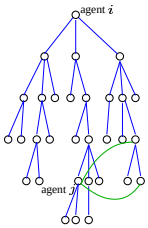
Nash equilibrium N $G = (V, E)$

Shortest path tree rooted at agent i

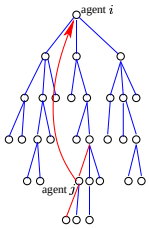


Cost(agent i) $\leq \alpha T_i + d(n-1)$ $T_i = \#$tree edges built by agent i

Cost of agent j

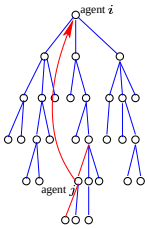


Cost of agent j



$\alpha T_j + \alpha$ + $(d+1)(n-1)$

Cost of agent j



Cost(agent j) $\leq \alpha T_j + \alpha$ + $(d+1)(n-1)$

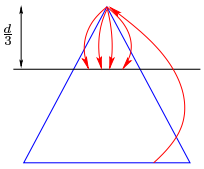
Cost Nash

Cost(agent i) $\leq \alpha T_i + d(n-1)$

Cost(agent j) $\leq \alpha T_j + \alpha + (d+1)(n-1)$

Cost(Nash eq.) $\leq \alpha(n-1) + \alpha(n-1) + (d+1)(n-1)n$

Analysis d



$d \leq \frac{3\alpha}{n^c}$ $\quad$ $c = \frac{1}{3}\left(\frac{\log \alpha}{\log n} + 1\right)$

Price of anarchy

Cost(Nash eq.) $\leq 2\alpha(n-1) + \left(\frac{3\alpha}{n^c} + 1\right)(n-1)n$

Cost(OPT) $\geq \alpha(n-1) + n(n-1)$

Open problems

Buffer management:

- Determine competitiveness of randomized algorithms.
- Packets have limited lifeliness.

Web caching

- Improve approximations guarantees.
- Complexity in the Uniform, Fault Models.

Network creation

- Settle price of anarchy of any α.
- Study other network creation games.

Generalized Linear Programming

Jiří Matoušek
Charles University, Prague

The cool slides in this presentation are included by the courtesy of Tibor Szabó.

Linear Programming

- Minimize cx subject to $Ax \le b$.
- Geometry: Minimize a linear function over the intersection of n halfspaces in R^d (=convex polyhedron).

LP Algorithms

- Simplex method [Dantzig 1947]
  - very fast in practice
  - very good "average case"
  - exponential-time examples for almost all pivot rules
- Ellipsoid method [Khachyian], interior-point methods [Karmakar],…
  - weakly polynomial but no (worst-case) bound in terms of n and d alone

Combinatorial LP algorithms

- wanted: time $\le f(d,n)$ for all inputs
- computations "coordinate independent"; use only combinatorial structure of the feasible set (polyhedron) or of the arrangement of bounding hyperplanes

Combinatorial LP algorithms

Computational geometry: research started with d fixed (and small)

- [Megiddo] $\exp(\exp(d)).n$
- [Clarkson] randomization; $d^2n+d^{d/2}\log n$
- [Seidel] simple randomized; $d!\,n$
- [Chazelle, M.] $\exp(O(d)).n$ deterministic
- parallel [Alon, Megiddo] [Ajtai, Megiddo]

A subexponential algorithm

Theory of convex polytopes (Hirsch conjecture): [Kalai] 1992	Computational geometry: [Sharir, Welzl], [M., Sharir, Welzl] 1992

$\exp(\sqrt{(d \log d)}).n$ (randomized expected)
- known as RANDOM FACET :
  In the current vertex of the feasible polytope, choose a random improving facet, recursively find its optimum, and repeat
- still the best known running time!

Abstract frameworks

- systems of axioms capturing some of the properties of linear programming
- running time of algorithms counted in terms of certain primitive operations
- to apply to a specific problem, need to implement them …
- … and then algorithms become available (such as Kalai/MSW, Clarkson)

Abstract frameworks

Abstract objective functions [Adler, Saigal 1976], [Wiliamson Hoke 1988], [Kalai 1988]
- P a (convex) polytope
- $f : V(P) \to R$ is an abstract objective function if a local minimum of any face F is also the unique global minimum of F
- every *generic* linear function induces an AOF
- but there are nonrealizable AOF on the 3-dimensional cube!

Abstract frameworks

Acyclic Unique Sink Orientations (AUSO)
- acyclic orientation of the graph of the considered polytope such that every nonempty face has exactly one sink (sink = all edges incoming)
- same as abstract objective functions

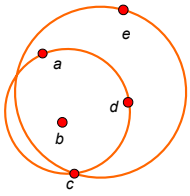
Abstract frameworks

LP-type problems [Sharir, Welzl]
- also called Generalized Linear Programs [Amenta]
- encompass many geometric optimization problems [MSW,Amenta,Halman…]
  - smallest enclosing ball of n points in R^d
  - smallest enclosing ellipsoid of n points in R^d
  - distance of two (convex) polyhedra in R^d
  - .....
- plus some non-geometric (games on graphs)

LP-type problems
- H a finite set of constraints
- $(W,\leq)$ a linearly ordered set (such as the reals)
- w: $2^H \to W$ a value function; intuitively: $w(G)$ is the minimum value of a solution attainable under the constraints in G
- Axiom M (monotonicity):
  If $F \subseteq G$, then $w(F) \leq w(G)$.
- Axiom L (locality):
  If $F \subseteq G$ and $w(F) = w(G) = w(F \cup \{h\})$, then $w(G) = w(G \cup \{h\})$.

Example: Smallest enclosing ball

- H a finite set of points in the plane
- $w(G)$ = radius of the smallest disk containing G



monotonicity trivial

locality depends on uniqeness of the smallest enclosing ball!

LP-type problems: more notions

- basis for G: inclusion-minimal $B \subseteq G$ with $w(B)=w(G)$
- dimension d of (H,w): maximum cardinality of a basis
- computational primitives (B a given basis)
  - violation test: value($B \cup \{h\}$)>value(G)?
  - pivoting: compute a basis for $B \cup \{h\}$

Abstract frameworks

Abstract Optimization Problems [Gärtner]

- only one parameter: dimension $d=|H|$ (no n)
- a linear ordering of 2^H
- primitive operation: Is G optimal among all sets containing F? If not, give a better G'
- nice randomized algorithm: $\exp(O(\sqrt{d}))$ [Gärtner]
- allows a (rather) efficient implementation of "primitives" in Kalai/MSW, e.g., for the smallest enclosing ball problem

Algorithms in the abstract frameworks

- several algorithms (Kalai/MSW = RANDOM FACET; Clarkson) work for AOF's, same analysis
  - AUSO given by oracle: returns edge orientations for a given vertex
  - yields $n.\exp(O(\sqrt{d}))$ randomized algorithm
  - analysis tight in this abstract setting [M.]
- for LP-type problems they work too (but…)
  - $O(n)$ algorithms for fixed d usually immediate
  - but primitives "depend on d" … may be hard
  - sometimes Gärtner's algorithm helps

Algorithms in the abstract frameworks

RANDOM EDGE

- the simplex algorithm that selects an improving edge uniformly at random
- for AUSO: random outgoing edge
- great expectations: perhaps always quadratic??? [Williamson Hoke 1988]

RANDOM EDGE

Expected running time

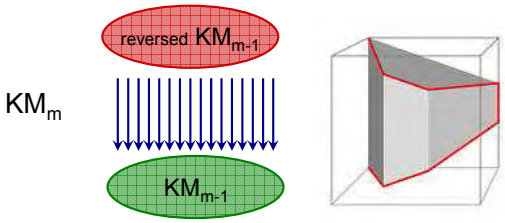
- on the d-dimensional simplex: $\Theta(\log d)$ [Liebling]
- on d-dimensional polytopes with d+2 facets: $\Theta(\log^2 d)$ [Gärtner et al. 2001]
- on the d-dimensional Klee-Minty cube:
  - $O(d^2)$ Williamson Hoke (1988)
  - $\Omega(d^2/\log d)$ Gärtner, Henk, Ziegler (1995)
  - $\Theta(d^2)$ Balogh, Pemantle (2004)

RANDOM EDGE can be (mildly) exponential

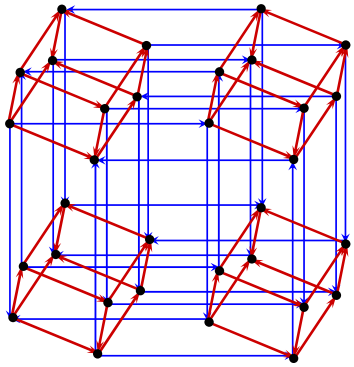
There exists an AUSO of the d-dimensional cube such that RANDOM EDGE, started at a random vertex, makes at least $\exp(c.d^{1/3})$ steps before reaching the sink, with probability at least $1- \exp(-c.d^{1/3})$.

[M., Szabó, FOCS 2004]

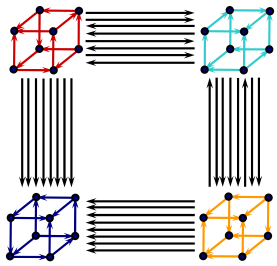
The Klee-Minty cube



A blowup construction



Hypersink reorientation

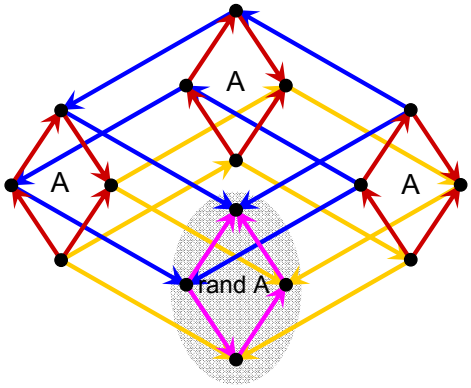


A simpler construction

Let A be a d-dimensional cube on which RANDOM EDGE is slow (constructed recursively)

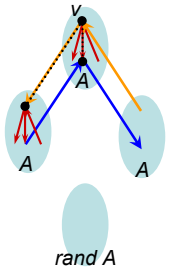
- take the blowup of A with random KM_m's whose sink is in the same copy of A, $m=\sqrt{d}$
- reorient the hypersink by placing a random copy of A
- thus, a step from d to $d+\sqrt{d}$

A simpler construction



A typical RANDOM EDGE move

- Move in the frame:
  - RANDOM EDGE move in KM_m
  - stay put in A
- Move within a hypervertex:
  - RANDOM EDGE move in A
  - move to a random vertex of KM_m on the same level



Random walk with reshuffles on KM_m
RANDOM EDGE on A

Walk with reshuffles on KM_m

- Start at a random $v^{(0)}$ *of* KM_m
- $v^{(i)}$ is chosen as follows:
  - with probability $p_{i,\text{step}}$ make a step of RANDOM EDGE from $v^{(i-1)}$;
  - with probability $p_{i,\text{resh}}$ randomly permute (reshuffle) the coordinates of $v^{(i-1)}$ to obtain $v^{(i)}$
  - with probability $1 - p_{i,\text{step}} - p_{i,\text{resh}}$, $v^{(i)} = v^{(i-1)}$.

Walk with reshuffles on KM_m is slow

Proposition. Suppose that

$$\min p_{i,resh} \geq 11 \cdot \max p_{i,step}$$

Then with probability at least $1 - e^{-\alpha m}$ the random walk with reshuffles makes at least $e^{\beta m}$ steps (α and β are constants).

Reaching the hypersink

- Either we reach the sink by reaching the sink of a copy of ***A*** and then perform RANDOM EDGE on KM_m. This takes at least $T(d)$ time.
- Or we reach the hypersink without entering the sink of any copy of A. That is, the random walk with reshuffles reaches the sink of KM_m. This takes at least $\exp(\beta m) \geq T(d)$ time.

The recursion

- RANDOM EDGE arrives to the hypersink at a random vertex. Then it needs $T(d)$ more steps. So passing from dimension d to $d+\sqrt{d}$ the expected running time of RANDOM EDGE doubles.
- Iterating $\sqrt{d}$ - times gives $T(2d) \geq 2^{\sqrt{d}}\, T(d)$.
- In order to guarantee that reshuffles are frequent enough we need a more complicated construction and that is why we are only able to prove a running time of $\exp(c.d^{1/3})$.

Open questions

- Obtain any reasonable upper bound on the running time of RANDOM EDGE
- Can one modify the construction such that the cube is realizable? (Probably not …)
- Or at least it satisfies the Holt-Klee condition?
- Or at least each three-dimensional subcube satisfies the Holt-Klee condition?

More open questions

- Find an algorithm for AOF on the d-cube better than $\exp(\sqrt{d})$
- The model of unique sink orientations of cubes (possibly with cycles) include LP on an arbitrary polytope.

  Find a subexponential algorithm!

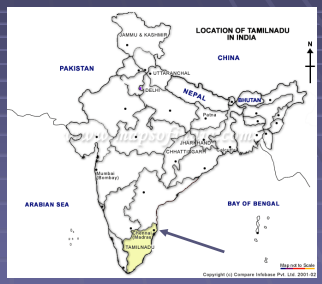
THE END

My Favorite Ten Complexity Theorems of the Past Decade II

Lance Fortnow
University of Chicago

Madras, December 1994

- Invited Talk at FST&TCS '04
- My Favorite Ten Complexity Theorems of the Past Decade



Why?

- Ten years as a complexity theorist.
- Looking back at the best theorems during that time.
- Computational complexity theory continually produces great work.
- Use as springboard to talk about research areas in complexity theory.
- Let's recap the favorite theorems from 1985-1994.

Favorite Theorems 1985-94 Favorite Theorem 1

- Bounded-width Branching Programs Equivalent to Boolean Formula
  - Barrington 1989

Favorite Theorems 1985-94 Favorite Theorem 2

- Parity requires $2^{\Omega(n^{1/d})}$ gates for circuits of depth d.
  - Håstad 1989

Favorite Theorems 1985-94 Favorite Theorem 3

- Clique requires exponentially large monotone circuits.
  - Razborov 1985

Favorite Theorems 1985-94 Favorite Theorem 4

- Nondeterministic Space is Closed Under Complement
  - Immerman 1988 and Szelepcsényi 1988

Favorite Theorems 1985-94 Favorite Theorem 5

- Pseudorandom Functions can be constructed from any one-way function.
  - Impagliazzo-Levin-Luby 1989
  - Håstad-Impagliazzo-Levin-Luby 1999

Favorite Theorems 1985-94 Favorite Theorem 6

- There are no sparse sets hard for NP via bounded truth-table reductions unless P = NP
  - Ogihara-Watanabe 1991

Favorite Theorems 1985-94 Favorite Theorem 7

- A pseudorandom generator with seed of length $O(s^2(n))$ that looks random to any algorithm using s(n) space.
  - Nisan 1992

Favorite Theorems 1985-94 Favorite Theorem 8

- Every language in the polynomial-time hierarchy is reducible to the permanent.
  - Toda 1991

Favorite Theorems 1985-94 Favorite Theorem 9

- PP is closed under intersection.
  - Beigel-Reingold-Spielman 1994

Favorite Theorems 1985-94
Favorite Theorem 10

- Every language in NP has a probabilistically checkable proof that can be verified with O(log n) random bits and a constant number of queries.
  - Arora-Lund-Motwani-Sudan-Szegedy 1992

Kyoto, March 2005

- Invited Talk at NHC Conference.
- Twenty years in field.
- My Favorite Ten Complexity Theorems of the Past Decade II

Derandomization

- Many algorithms use randomness to help searching.
- Computers don't have real coins to flip.
- Need strong pseudorandom generators to simulate randomness.

Hardness vs. Randomness

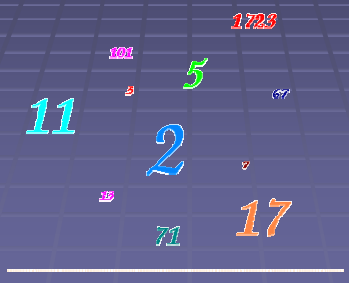
- BPP – Class of languages computable efficiently by probabilistic machines
- 1989 – Nisan and Wigderson
  - If exponential time does not have circuits that cannot solve EXP-hard languages on average then P = BPP.
- Many extensions leading to …

Favorite Theorem 1

- If there is a language computable in time $2^{O(n)}$ that does not have $2^{\varepsilon n}$-size circuits then P = BPP.
  - Impagliazzo-Wigderson '97

Primality

- How can we tell if a number is prime?



Favorite Theorem 2

- Primality is in P
  - Agrawal-Kayal-Saxena 2002

Complexity of Primality

- Primes in co-NP: Guess factors
- Pratt 1975: Primes in NP
- Solovay-Strassen 1977: Primes in co-RP
- Primality became the standard example of a probabilistic algorithms
- *Primality is a problem hanging over a cliff above P with its grip continuing to loosen every day.* – Hartmanis 1986

More Prime Complexity

- Goldwasser-Kilian 1986
- Adleman-Huang 1987
  - Primes in RP: Probabilistically generate primes with proofs of primality.
- Fellows-Kublitz 1992: Primes in UP
  - Unique witness to primality
- Agrawal-Kayal-Saxena – Primes in P

Division

- Division in Non-uniform Logspace
  - Beame-Cook-Hoover 1986
- Division in Uniform Logspace
  - Chiu 1995
- Division in Uniform NC_1
  - Chiu-Davida-Litow 2001
- Division in Uniform TC_0
  - Hesse 2001

Probabilistically Checkable Proofs

- From 1994 list:
  - Every language in NP has probabilistically checkable proof (PCP) with O(log n) random bits and constant queries.
  - Arora-Lund-Motwani-Sudan-Szegedy
- Need to improve the constants to get stronger approximation bounds.

Favorite Theorem 3

- For any language L in NP there exists a PCP using O(log n) random coins and 3 queries such that
  - If x in L verifier will accept with prob $\geq 1-\varepsilon$.
  - If x not in L verifier will accept with prob $\leq \frac{1}{2}$.
- Håstad 2001

Approximation Bounds

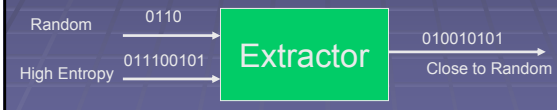
- Given a 3CNF formula we can find assignment that satisfies 7/8 of the clauses by choosing random assignment.
- By Håstad can't do better unless P = NP.
- Uses tools of parallel repetition and list decodable codes that we will see later.

Connections

- Beauty in results that tie together two seemingly different areas of complexity.

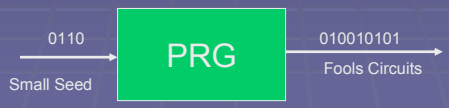
Connections

- Beauty in results that tie together two seemingly different areas of complexity.
- Extractors – Information Theoretic



Connections

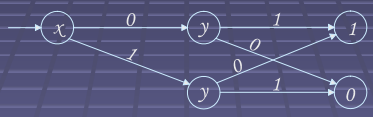
- Beauty in results that tie together two seemingly different areas of complexity.
- Extractors – Information Theoretic
- Pseudorandom Generators - Computational



Favorite Theorem 4

- Equivalence between PRGs and Extractors.
- Allows tools for one to create other, for example Impagliazzo-Wigderson to create extractors.
  - Trevisan 1999

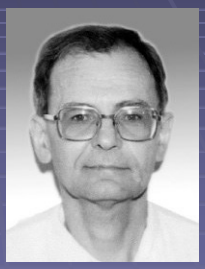
Superlinear Bounds



- Branching Programs
  - Size corresponds to space needed for computation.
  - Depth corresponds to time.
- We knew no non-trivial bounds for general branching programs.

Favorite Theorem 5

- Non-linear time lower bound for Boolean branching programs.
- Natural problem that any linear time algorithm uses nearly linear space.
- Ajtai 1999



Parallel Repetition

0110

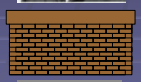
1010

1100

1001

Accepts with prob ½

Parallel Repetition



0110 0010

1010 1011

1100 0100

1001 1011

Accepts with prob 1/4

Parallel Repetition

FALSE

0110 0010

1010 1011

1100 0100

1001 1011

Accepts with prob 1/4

Favorite Theorem 6

- Parallel Repetition does reduce error exponentially in number of rounds.
- Useful in construction of optimal PCPs.
- Raz 1998

List Decoding

00101110

List Decoding

00101110

0100011001010011100101010101110011101111110001110

List Decoding

00101110

0100011001010011100101010101110011101111110001110

List Decoding

00101110

0100011001010011100101010101110011101111110001110

00101110

List Decoding

00101110

0100011001010011100101010101110011101111110001110

List Decoding

00101110

0100011001010011100101010101110011101111110001110

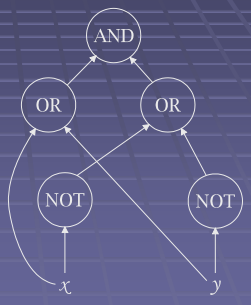
10010010
00101110
10111000
11101110

Favorite Theorem 7

- List Decoding of Reed-Solomon Codes Beyond Classical Error Bound
  - Sudan 1997
- Later Guruswami and Sudan gives algorithm to handle believed best possible amount of error.

Learning Circuits

- Can we learn circuits by making equivalence queries, i.e., give test circuit and get out counterexample.
- No unless we can factor.



Favorite Theorem 8

- Can learn circuits with equivalence queries and ability to ask SAT questions.
  - Bshouty-Cleve-Gavaldà-Kannon-Tamon 1996

Corollaries

- If SAT has small circuits, we can learn circuit for SAT with SAT oracle.
- If SAT has small circuits then PH collapses to ZPP^{NP}.
  - Köbler-Watanabe

Quantum Lower Bounds

0100

10001

00010010

10001000

Quantum Lower Bounds

0100

10001

00010010

10001000

Favorite Theorem 9

- Razborov 2002
  - $N^{1/2}$ quantum bits required to compute set disjointness, i.e., whether the two strings have a one in the same position.
  - Matches upper bound by Buhrman, Cleve and Wigderson.

Derandomizing Space

- Given a randomized log n space algorithm can we simulate it in deterministic space?
- Simulate any randomized algorithm in $\log^2 n$ space.
  - Savitch 1969

Favorite Theorem 10

- Saks-Zhou 1999
  - Randomized log space can be simulated in deterministic space $\log^{3/2} n$.

Conclusions

- Complexity theory has had a great decade producing many ground-breaking results.
  - Every theorem builds on other work.
  - Wide variety of researchers from a cross section of countries.
- New techniques still needed to tackle the big separation questions.

The Next Decade

- Favorite Theorem 1
  - Undirected Graph Connectivity in Deterministic Logarithmic Space
  - Reingold 2005

March 3, 2005

Some Heuristic Analysis of Average Behavior of Local Search Algorithms

Osamu Watanabe
Dept. of Math. & Comp. Sci., Tokyo Institute of Technology
http://www.is.titech.ac.jp/~watanabe/smapip/

Abstract
We propose some *Heuristic Approach* for analyzing average performance of local search algorithms. As an example, we consider some satisfiability problems and invesitgate local search algorithms for them.

Sorry!
- No theorem
- ⟶ Some proposal
  Small observations
- No animation
- No color

1. Motivation: Experiments ⟹ ? ⟹ Rigorous Analyses

Facts
- Some problems, though they are believed hard in the worst case, are solvable "efficiently" *on average* by relatively simple algorithms.
- Most of the positive results are given by computer experiments.

Why Analysis? *Computer experiments are not enough!?*
- More efficient than running the algorithm for many times.
- For better understanding of the feature/principle of the algorithm, which may leads us to improvements/applications to other problems.

But rigorous analysis is difficult!!

What shall we do!?

Our Strategy

ANALYSYS ⟸ { 1. *bra bra bra* ; 2. *are kore* ; 3. *nan ya kan ya* }
⇑
need experiments on some step

Remarks.
- There are some strong mathematical techniques developed in different fields of mathematical sciences, e.g., *statistical physics*, which have been also applied for analyzing average case performance of such algorithms.
  ⇒ But these approaches are not perfect:
  e.g., analysis for $n \to \infty$ or $t \to \infty$ may not be sufficient.
- Some rigorous analyses have been reported also in computer science.
  ⇒ But there are still some limitations:
  e.g., applicable to a certain class of algorithms.

2. Our Approach for Analyzing Local Search Algorithms

Motivation:
- Many contraint satisfaction problems can be solved *to some extent* by local search algorithms *on average*.
- Local search algorithm is not unique! There are many variations.

Our Approach [Watanabe-etal, SAGA'03]:
0. Modify an algorithm to a randomized one.
1. Define a relatively simple Markov process that simulates (reasonably well) the execution of the algorithm.
2. Approximate *average states* of this process by a relatively simple formula.

Remarks.
0. ⇐ This may lose some efficiency, but it reduces dependency to paricular inputs.
1. ⇐ This may be hard to justify.
2. ⇐ We have some justification for this approximation.

3. First Example

Problem: 3-⊕-SAT (Parity SAT)

Closest Solution Search for 3-⊕-SAT

Input: (1) 3-⊕-SAT formula F over variables $x_1, ..., x_n$.
(2) Assignment $\boldsymbol{a}$.

Output: A sat. assignment that is closest to $\boldsymbol{a}$.

3-⊕-SAT formula = a conjunction of *parity clauses*
$F = (\neg x_3 + x_7 + x_2) \wedge (x_1 + \neg x_{12} + \neg x_{61}) \wedge \cdots$

Average Case Senario: Random Positive $(3,6)$-⊕-SAT Formulas
(1) Every variable appears 6 times in F; hence, # of clauses $= 2n$.
(2) Sings are chosen uniformly at randomly so that $\mathbf{0}$ becomes a solution.
(3) An initial assignment $\boldsymbol{a}$ is chosen uniformly at random from those with Hamming distance pn from $\mathbf{0}$; that is, $\boldsymbol{a}$ has pn 1's.

Remarks.
- Essentially the same as the Decoding Problem for Linear Codes.
- A solution search for ⊕-SAT is poly. time computable.

$$x_3 + x_7 + x_2 = 1, \quad x_1 + x_{12} + x_{61} = 0, \quad \ldots$$

- The closest solution search is NP-hard.

... But $\boldsymbol{a}$ is regarded as a *hint* !?

Algorithm: Local Search Algorithm; Greedy (or Steepest Decending Method?)

Local Search Algorithm for $(3,6)$-⊕-SAT

program `GreedyPSAT`(F, $\boldsymbol{a}$);
  $\mathtt{x}_1, ..., \mathtt{x}_n \leftarrow \boldsymbol{a}$;
  repeat the following MAXT steps
    if F is satisfied with $\vec{\mathtt{x}}$ **then** output the current assignment and halt;
    flip the value of $\mathtt{x}_i$ with the highest$^{(\star)}$ penalty;
program end.
(*) If there are several, choose one in some determinisitic way.

penalty of $\mathtt{x}_j$ = # of unsatisfied clauses containing $\mathtt{x}_j$.

Remarks.
- Each $\mathtt{x}_j$ appears 6 times. Thus, $0 \le$ Penalty of $\mathtt{x}_j \le 6$.
- Fix MAXT $= 2pn$, where $Ham(\boldsymbol{a}, \mathbf{0}) = pn$. Use $n = 6000$.

This works quite well !!

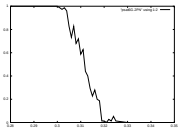


Fig 1. The success prob. vs. p
Recall p is the parameter for the init. Ham. distance $Ham(\boldsymbol{a}, \mathbf{0}) = pn$.

By using larger bounds, the success threshold gets increased; but not so much, and seems to have some limit.

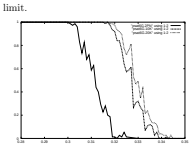


Fig 2. The success prob. vs. p
MAXT $= 2pn (\approx 3600)$, 10000, and 20000

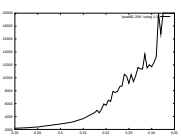


Fig 3. average steps vs. p

For Understanding the Success Threshold

How does the Ham. distance change *on average*?

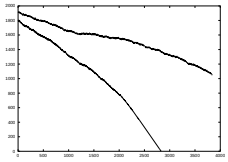


Fig 4. Ham. distance vs. step t for some execution, $p = 0.30$ and $p = 0.32$

Technical Goal: State the following function (or its approximation) in a simple form.

$$err_p(t) \;=\; \text{the average Ham. distance from the solution after the } t\text{th step.}$$

Our Approach

Step 0. Modify the algorithm to a randomized one.

program `GreedyPSAT`(F, $\boldsymbol{a}$);
  $\mathtt{x}_1, ..., \mathtt{x}_n \leftarrow \boldsymbol{a}$;
  repeat the following MAXT steps
    if F is satisfied with $\vec{\mathtt{x}}$ **then** output the current assignment and halt;
    flip the value of $\mathtt{x}_i$ with the highest$^{(*)}$ penalty;
program end.

$\Downarrow$

program `SoftGreedyPSAT`(F, $\boldsymbol{a}$);
  $\mathtt{x}_1, ..., \mathtt{x}_n \leftarrow \boldsymbol{a}$;
  repeat the following MAXT steps
    if F is satisfied with $\vec{\mathtt{x}}$ **then** output the current assignment and halt;
    choose $\mathtt{x}_i$ randomly according to their weights$^{(*)}$;
    flip the value of $\mathtt{x}_i$;
program end.

How to Choose $\mathtt{x}_j$?

$$\Pr[\,\mathtt{x}_j \text{ is chosen}\,] \;=\; \frac{W(\text{penalty of } \mathtt{x}_j)}{\text{total weiths}},$$

where W is set, e.g., as follows for $n = 6000$,

$$W(0) = 0,\;\; W(1) = 1,\;\; W(2) = 100,\;\; W(3) = 10000,$$
$$W(4) = 100000,\;\; W(5) = 500000,\;\; W(6) = 2500000.$$

Our Approach, Cont.

Step 1. Define a simple Markov process simulating the algorithm.

Remark.
The execution of the algorithm is indeed a Markov chain with the following state space:

$$\{\ (y_1, ..., y_n)\ :\ y_j \in \{0, 1\}\ \} \quad\leftarrow\quad \text{the set of assignments to variables } \mathtt{x}_j.$$

But this is too big!
$\Downarrow$ state space reduction
A simple Markov process

***** first idea *****

Use a tuple $(n_{+,0}, ..., n_{+,6}, n_{-,0}, ..., n_{+,6})$ of numbers such that

$$n_{+,k} \;=\; \#\text{ of correctly assigned variables with penalty } k.$$

Regard the execution of the algorithm as the change of this state by the following transition rule:

1. Choose $sg \in \{+, -\}$ and k, $1 \le k \le 6$, with prob. $P(sg, k)$, where
$$P(sg, k) \;=\; \frac{W(k) \cdot n_{sg,k}}{\sum_{\ell=1}^{6} W(k) \cdot (n_{+,k} + n_{-,k})} \quad\left(\;=\; \frac{W(k) \cdot n_{sg,k}}{\text{total weights}}\right).$$
2. Update the current state by
$$\begin{array}{rcl} n_{sg,k} & \to & n_{sg,k} - 1 \\ n_{sg,6-k} & \to & n_{-sg,6-k} + 1 \end{array}$$
3. Futher update the state for reflecting the staus change of *related* variables.

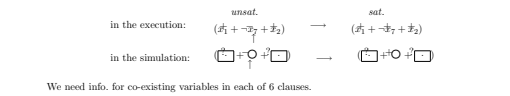
Remarks. $\boldsymbol{n}_t = (n^{(t)}_{+,0}, ..., n^{(t)}_{+,6}, n^{(t)}_{-,0}, ..., n^{(t)}_{-,6})$

- The total number is $\sum_{\ell=0}^{6} n^{(t)}_{+,\ell} + n^{(t)}_{-,\ell} = n\ (= 6000)$.
- The Ham. distance is $err_p(t) = \sum_{\ell=0}^{6} n^{(t)}_{-,\ell}$.
- An initial state $\boldsymbol{n}_0 = (n^{(0)}_{+,0}, ...)$ can be estimated by p.
  But here we will use the values for some randomly generated instance.

Unfortunately, this state space is too simple.

1. Choose $sg \in \{+, -\}$ and k, $1 \le k \le 6$, with prob. $P(sg, k)$.
2. Update the current state by changing $n_{sg,k}$ and $n_{sg,6-k}$.

⇒3. Futher update the state for reflecting the staus change of *related* variables.



We need info. for co-existing variables in each of 6 clauses.

$n_{\pm,(i)}$ = # of variables assigned (in)correctly $(+/-)$ that appears in 6 clauses assigned of pattern i,
where $i = 1 \sim 56$ (effective ones are ≤ 20).

$(x,+,+)$ $(x,+,+)$
$(x,+,-)$ $(x,+,-)$
$(x,+,-)$ $(x,-,-)$
assignment pattern

Express the state of the execution by using these $112 = 2 \times 56$ numbers.

Then the simulation matches the execution quite well !

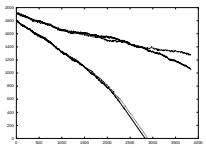


Fig 5. Ham. distance vs. step t: simulation and execution, $p = 0.30$ and $p = 0.32$

Assume that this simulation is accurate enough.

Then the analysis becomes feasible.

Our Approach, Cont.

Step 2. Approximate this random process by a simple recurrence formula.

$$\mathrm{E}[\,\boldsymbol{n}_t\,] \;\approx\; f^t(\boldsymbol{n}_0).$$
$$\Downarrow$$
$$err_p(t) \;=\; \mathrm{E}[\textstyle\sum_i n^{(t)}_{-,(i)}\,] \;\approx\; Sum_-(f^t(\boldsymbol{n}_0)) \stackrel{def}{=} approx\text{-}err_p(t)$$

Then by analyzing $approx\text{-}err_p(t)$, we can observe that a gap exists when the execution reaches to a stage where no variable with penalty ≥ 4 exist.

Remarks.

- By make a flip on a penalty k variable, the total penalty gets decreased by $k - 3$.

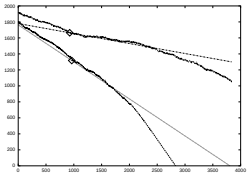


Fig 6. (average) derivative at the beginning of stage 3

Is it Enough ?

Am I Happy ? No !

$$\mathrm{E}[\boldsymbol{n}_t] \approx f^t(\boldsymbol{n}_0).$$

The function f is "relatively" simple. But...
Currently, f is expressed as a program with several hundred lines!
f is a formula on 40 variables :-(

• • •

4. Second Example

Problem: 3-SAT (CNF SAT)

Input: 3-CNF formula F over variables $x_1, ..., x_n$.
Output: A sat. assignment.

Average Case Senario: Random Positive $(3, d)$-SAT Formulas
(1) Every variable appears d times in F; hence, # of clauses $= dn/3$.
(2) Sings are chosen uniformly at randomly so that $\mathbf{0}$ becomes a solution.

Algorithm: Local Search Algorithm; Random Walk (often called *WALKSAT*)

Local Search Algorithm for $(3, d)$-SAT

program `RandomWalkSAT`(F);
  $\mathtt{x}_1, ..., \mathtt{x}_n \leftarrow$ randomly chosen $\boldsymbol{a}$ in $\{0,1\}^n$;
  repeat the following MAXT steps
    if F is satisfied with $\vec{\mathtt{x}}$ **then** output the current assignment and halt;
    choose one unsat. clause and select one of the three variables in it;
    make a flip on the selected variable;
  program end.

Cf.

program `GreedySAT`(F);
  $\mathtt{x}_1, ..., \mathtt{x}_n \leftarrow$ randomly chosen $\boldsymbol{a}$ in $\{0,1\}^n$;
  repeat the following MAXT steps
    if F is satisfied with $\vec{\mathtt{x}}$ **then** output the current assignment and halt;
    choose one variable with the highest penalty;
    make a flip on the selected variable;
  program end.

Why not Greedy ?

Easy Answer:
Because it does not work.
Usually trapped by a local minimum.

No Problem !!

program `SoftGreedySAT`(F);
  $\mathtt{x}_1, ..., \mathtt{x}_n \leftarrow$ random $\boldsymbol{a}$;
  repeat the following MAXT steps
    if F is satisfied with $\vec{\mathtt{x}}$ **then** output the current assignment and halt;
    choose $\mathtt{x}_i$ randomly according to their weights;
    flip the value of $\mathtt{x}_i$;
  program end.

In fact, *e.g.*, for $(3, 6)$-SAT and $n = 6000$,

RandomWalkSAT $\leftrightarrow$ $W[0] = 0$, $W[1] = 1$, ..., $W[6] = 6$.
SoftGreedySAT $\leftrightarrow$ $W[0] = 0$, $W[1] = 1$, $W[2] = 20$, ..., $W[6] = 20^5$.

Second Answer:
Not so much difference.

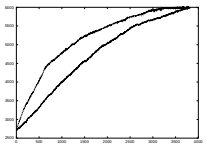


Fig 7. $n_0 = \#$ of penalty 0 var.s
SoftGreedy vs. RandomWalk

Remark.
Penalty 0 variables are those appearing only in sat. clauses.

For Understanding the Behavior

$\Longrightarrow$ Simulation by a Simple Markov Process

A similar but slightly different set of parameters is used.

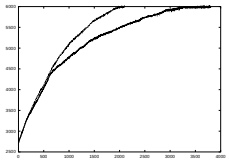


Fig 8. $n_0 = \#$ of penalty 0 var.s
Simulation vs. SoftGreedy

What does make this difference ?

Maybe the correlation between flipped variables.

$\Downarrow$ then

What if a flip is restricted only once ?

It works !!

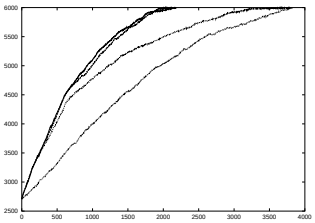


Fig 8. n_0 = # of penalty 0 var.s
Simulation, SoftGreedy (flip once), SoftGreedy, and RandomWalk

Remarks.

- Usually a solution cannot be obtaind under the flip-once restriction. But an assignment, after running out all unflipped variables (with penalty > 0), gets close enough to some solution.
- We cannot always hope this nice property. This algorithmic trick works for $d \leq 8$.

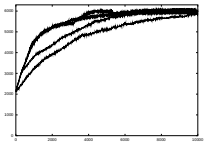


Fig 9. $(3, 8)$-SAT

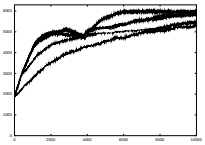


Fig 10. $(3, 9)$-SAT

5. Concluding Remarks

1. An Heuristic Analysis (Real exec. → Simple process)
⇒ Some reasoning for the success threshold
⇒ An improvement of the algorithm

2. Some Observations (On Local Search Algorithms)
(1) Greedy is fast, but it needs to get a solution (or something very close to it) before running out high penalty variables.
(2) There seems some other reasoning for RandomWalk.